



3e Technologies International, Inc.
FIPS 140-2
Non-Proprietary Security Policy
Level 2 Validation
For 3e-525A, 3e-525N and 3e-519

Version 6.5

Dec 27, 2004

Copyright ©2004 by 3e Technologies International.
This document may freely be reproduced and distributed in its entirety.

GLOSSARY OF TERMS.....	3
1. INTRODUCTION.....	4
1.1. PURPOSE	4
1.2. DEFINITION	5
1.3. SCOPE	6
2. ROLES, SERVICES, AND AUTHENTICATION.....	7
2.1.1. Roles and Services	7
2.1.2. Authentication Mechanisms and Strength	11
3. SECURE OPERATION AND SECURITY RULES	12
3.1. SECURITY RULES	12
3.2. PHYSICAL SECURITY RULES	12
3.3. SECURE OPERATION INITIALIZATION	16
3.3.1. System Configuration.....	18
3.3.2. Wireless Configuration	21
3.3.3. NCAP Configuration (for 3e-525N only).....	27
3.3.4. Services Settings.....	32
3.3.5. User Management.....	36
3.3.6. System Administration	38
4. SECURITY RELEVANT DATA ITEMS	41
4.1. CRYPTOGRAPHIC ALGORITHMS	41
4.2. SELF-TESTS	41
4.3. CRYPTOGRAPHIC KEYS AND SRDIs.....	42
4.4. ACCESS CONTROL POLICY	43
5. OPERATIONAL ENVIRONMENT.....	44
6. EMI/EMC.....	44
7. DESIGN ASSURANCE.....	44
8. MITIGATION OF OTHER ATTACKS	44

Glossary of terms

AP	Access Point
CO	Cryptographic Officer
DAQ	Data Acquisition
DH	Diffie Hellman
DHCP	Dynamic Host Configuration Protocol
DMG	Dual Mode Gateway
IP	Internet Protocol
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
HTTPS	Secure Hyper Text Transport Protocol
LAN	Local Area Network
MAC	Medium Access Control
NCAP	Network Capable Application Processor
NAT	Network Address Translation
PRNG	Pseudo Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SRDI	Security Relevant Data Item
SSID	Service Set Identifier
TLS	Transport Layer Security
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

1. Introduction

1.1. Purpose

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International's wireless gateway products, the *3e-525A*, *3e-519* and *3e-525N Wireless Gateway* (HW P/Ns 3e-525A, 3e-519 and 3e-525N; Firmware Version 3.0), hereafter known as the 3e-DMG (Dual Mode Gateway). This policy was created to satisfy the requirements of FIPS 140-2 Level 2. This document defines 3eTI's security policy and explains how the 3e-DMG Wireless Gateways meet the FIPS 140-2 security requirements.

The figures below show the 3e-525A, 3e-519 and 3e-525N Wireless Gateways.



Figure A: 3e-525A Wireless Gateway

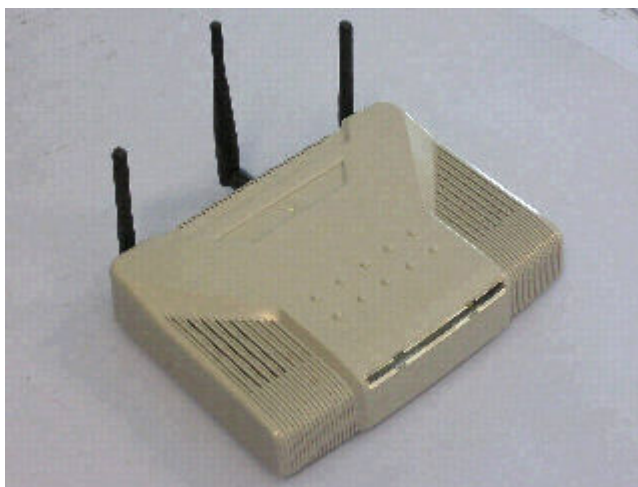


Figure B: 3e-519 Wireless Gateway



Figure C: 3e-525N Wireless Gateway

The cryptographic module security policy consists of a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard. Please refer to FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules* available on the NIST website at <http://csrc.nist.gov/cryptval/>.

1.2. Definition

The 3e-DMG Wireless Gateway is device which consists of electronic hardware, embedded software and strong metal case or plastic physical enclosure. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The 3e-DMG gateway operates as either a gateway connecting a local area network to wide area network (WAN) or as an access point within a local area network (LAN). The cryptographic boundary of the 3e-DMG Gateway is defined to be the entire enclosure of the Gateway. The 3e-DMG is physically bound by the mechanical enclosure which is protected by tamper evident tape.

3eTI Gateway software provides the following major services in FIPS mode:

- Wireless 802.11b Access Point functionality (bridging from the wired uplink LAN to the wireless LAN).
- Wireless 802.11b/g bridge functionality
- DHCP service to the local LAN (allows a wired local LAN to exist over the local LAN interface).
- SNMP*
- USB printer services (For 525A and 519 only)
- Subnet Roaming
- DAQ modules I/O (For 525N only)

* Although SNMP traffic is transmitted encrypted (using DES or AES), for FIPS purposes, it is considered to be plaintext. The reason being, encryption keys are derived from a pass-phrase, which is not allowed in FIPS mode.

1.3. Scope

This document will cover the secure operation of the 3e-DMG including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and describe the Security Relevant Data Items (SRDIs).

The Gateway has four modes of operations which are listed in the table below:

Mode	FIPS Mode
Gateway Mode (Mode 1)	No
Gateway Mode (Mode 2)	Yes
AP / Bridging Mode (Mode 1)	No
AP /Bridging Mode (Mode 2)	Yes

The Gateway – FIPS mode (Mode 2) and AP/Bridging - FIPS mode (Mode 2) are explained in this document. The other modes cannot be validated to FIPS 140-2 because they execute applications that use non-FIPS Approved cryptographic algorithms.

In order to enter FIPS mode, select the FIPS 140-2 Mode box on the Operation Mode page of the management GUI (see 3.3.1.3). This will force the gateway to return to factory defaults and then the gateway will reboot into FIPS mode. To leave FIPS mode, un-select the FIPS 140-2 Mode box and apply the changes. Once again, the gateway will restore factory defaults and then reboot into non-FIPS mode.

On transition between modes, the system is returned to factory defaults and all keys are zero-ized.

2. Roles, Services, and Authentication

The 3e-DMG supports four separate roles. The set of services available to each role is defined in this section. The 3e-DMG authenticates an operator's role by verifying his PIN or access to a shared secret.

2.1.1. Roles and Services

The 3eTI gateway supports the following authorized roles for operators:

Crypto Officer Role: The Crypto officer role performs all security functions provided by the Gateway. This role performs cryptographic initialization and management functions (e.g., module initialization, input/output of cryptographic keys and SRDIs, audit functions and user management). The Crypto officer is also responsible for managing the Administrator users. The Crypto officer must operate within the Security Rules and Physical Security Rules specified in Sections 3.1 and 3.2. The Crypto officer uses a secure web-based HTTPS connection to configure the Gateway. Only one Crypto Officer is defined in the Gateway. The Crypto Officer authenticates to the Gateway using a username and password.

Administrator Role: This role performs general Gateway configuration such as defining the WLAN, LAN and DHCP settings, performing self-tests and viewing system log messages for auditing purposes. No CO security functions are available to the Administrator. The Administrator can also reboot the Gateway if deemed necessary.

The Administrator must operate within the Security Rules as specified in Section 3.1 and always uses a secure web-based HTTPS connection to configure the Gateway. The Administrator authenticates to the Gateway using a username and password. Up to 5 operators who can assume the Administrator role can be defined. All Administrators are identical i.e. they have the same set of services available. The Crypto Officer is responsible for managing (creating, deleting) Administrator users.

The follow table outlines the functionalities that are provided by each role:

Categories	Features	Operator Roles											
		CryptoOfficer						Administrator					
		Show ¹	Set ²	Add ³	Delete ⁴	Zeroize ⁵	Default Reset ⁶	Show ⁷	Set ⁸	Add ⁹	Delete ¹⁰	Zeroize ¹¹	Default Reset ¹²
System Configuration													
• General	Hostname	X	X				X	X	X				X
	Domain name	X	X				X	X	X				X
	Date/Time	X	X				X	X	X				X
• WAN	DHCP client	X	X				X	X	X				X
	Static IP address	X	X				X	X	X				X
	10/100 MBps half/full duplex/auto	X	X				X	X	X				X
• LAN	IP address	X	X				X	X	X				X
	Subnet mask	X	X				X	X	X				X
• Operating Mode	Gateway – FIPS	X	X				X	X	X				X
	Gateway – Non-FIPS	X	X				X	X	X				X
	AP / Bridging Mode – FIPS	X	X				X	X	X				X
	AP / Bridging Mode – Non-FIPS	X	X				X	X	X				X
	AP / Bridging Mode – FIPS / IPv6	X	X				X	X	X				X
	AP / Bridging Mode – Non-FIPS / IPv6	X	X				X	X	X				X
Wireless Configuration													
• General	SSID	X	X				X	X	X				X
	Channel Number	X	X				X	X	X				X
	• Enable / Disable Auto Selection	X	X				X	X	X				X
	• Auto selection button	X	X				X	X	X				X
	Transmit Power Mode	X	X				X	X	X				X
	Fixed Power Level	X	X				X	X	X				X
	Beacon Interval	X	X				X	X	X				X
	RTS Threshold	X	X				X	X	X				X
	DTIM	X	X				X	X	X				X
	Basic Rates	X	X				X	X	X				X
	Preamble	X	X				X	X	X				X

¹ The operator can view this setting

² The operator can change this setting

³ The operator can add a required input. For example: Adding an entry to the MAC address filtering table

⁴ The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table

⁵ The operator can zeroize these keys.

⁶ The operator can reset this setting to its factory default value. This is done by performing a zeroize

⁷ The operator can view this setting

⁸ The operator can change this setting

⁹ The operator can add a required input. For example: Adding an entry to the MAC address filtering table

¹⁰ The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table

¹¹ The operator can zeroize these keys.

¹² The operator can reset this setting to its factory default value. This is done by performing a zeroize

Categories	Features	Operator Roles											
		CryptoOfficer						Administrator					
		Show ¹	Set ²	Add ³	Delete ⁴	Zeroize ⁵	Default Reset ⁶	Show ⁷	Set ⁸	Add ⁹	Delete ¹⁰	Zeroize ¹¹	Default Reset ¹²
	Enable / Disable Broadcast SSID	X	X				X	X	X				X
• Encryption	No Encryption	X	X				X						X
	Dynamic Key Management	X	X				X						X
	3DES	X	X			X	X						X
	AES (128-/192-256-bit)	X	X			X	X						X
• Bridging	Wireless Mode	X	X				X	X	X				X
	Spanning Tree Protocol	X	X				X	X	X				X
	Channel No	X	X				X	X	X				X
	Tx Pwr Mode	X	X				X	X	X				X
	Bridge signal strength LED port	X	X				X	X	X				X
	Add/Remove Remote AP's BSSID	X	X				X	X	X				X
• Encryption	No Encryption	X	X				X						X
	3DES	X	X		X	X	X						X
	AES (128-/192-256-bit)	X	X		X	X	X						X
• MAC Address Filtering	Enable/Disable	X	X				X	X					X
	Add/Delete entry			X	X								
	Allow/Disallow Filter	X	X				X	X					X
• Rogue AP Detection	Enable/Disable	X	X				X	X	X				X
	Known AP MAC address			X	X								
	Email / Display rogue AP	X	X				X	X	X				X
NCAP Configuration (3e-525N only for this section)													
• General	Node information	X	X				X	X	X				X
	Enable Error Log	X	X				X	X	X				X
• DAQ Modules	DAQ Module Information	X	X		X		X	X	X		X		X
• Physical Channels	DAQ Channel Parameters	X	X				X	X	X				X
• Virtual Channels	DAQ Virtual Channel Parameters	X	X	X			X	X	X	X			X
• Communication Modules	Enable/ Disable	X	X				X	X	X				X
• Application Control	Enable / Disable	X	X				X	X	X				X
Service Settings													
• DHCP Server	Enable / Disable	X	X				X	X	X				X
	Starting / Ending IP address	X	X				X	X	X				X
• Subnet Roaming	Enable / Disable	X	X				X	X	X				X
	Coordinator Address	X	X		X		X	X	X	X			X
• Print Server	Enable/ Disable	X	X				X	X	X				X
• SNMP agent	Enable/ Disable	X	X				X	X	X				X
	Community settings	X	X				X	X	X				X
	Secure User Configuration	X	X				X	X	X				X
	System Information	X	X				X	X	X				X
User Management													
• List All Users		X		X	X		X	X					X
• Add New User			X										
• User Password Policy	Enable/Disable	X	X				X						X
	Policy setting												
Monitoring/Reports													

Categories	Features	Operator Roles											
		CryptoOfficer						Administrator					
		Show ¹	Set ²	Add ³	Delete ⁴	Zeroize ⁵	Default Reset ⁶	Show ⁷	Set ⁸	Add ⁹	Delete ¹⁰	Zeroize ¹¹	Default Reset ¹²
• System Status	Security Mode Current Encryption Mode Bridging encryption mode System Uptime Total Usable memory Free Memory Current Processes Other Information Network interface status	X X X X X X X X X						X X X X X X X X X					
• Bridging Status	Status of Layer 2 bridge devices	X						X					
• Wireless Clients	MAC Address (manfr’s name) Received Signal Strength TX rate	X X X						X X X					
• Adjacent AP List	AP MAC address SSID Channel Signal Noise Type Age WEP	X X X X X X X X						X X X X X X X X					
• DHCP Client List	Client Hostname IP Address MAC Address (manfr’s name)	X X X			X X X			X X X			X X X		
• System Log	Date/Time/Message	X			X			X			X		
• Web Access Log		X			X			X			X		
• Network Activities		X			X			X			X		
System Administration													
• Firmware Upgrade		X											
• Self-Test		X						X					
• Factory Defaults		X											
• Reboot		X						X					
• Utilities	Ping Traceroute	X X						X X					

User Role: This role is assumed by the wireless client workstation that uses static or dynamic key AES or 3DES encryption to communicate wirelessly with the Gateway AP. Authentication is implicitly selected by the correct knowledge of the static key, or for dynamic key encryption, EAP-TLS authentication is performed and the client uses its public key certificate to authenticate itself. The static key (TDES or AES key) is configured on the Gateway by the Crypto officer. The static key must be pre-shared between the Gateway and User. The Gateway supports 128 Users (client workstations) if

MAC address filtering is disabled. If MAC address filtering is enabled, only 60 Users are allowed.

The only service available to the User role is the ability to send data to and through the 3e-DMG. All data is sent in the form of 802.11b wireless packets. All wireless communication is encrypted using either 3DES or AES encryption (based upon Gateway configuration). In bypass mode plaintext packets can also be sent to the Gateway

Security Server Role: This role is assumed by the authentication server, which is a self-contained workstation connected to the Gateway over the Ethernet Uplink WAN port. The security server is employed for authentication of wireless clients and key management activities. The Security Server is used only during dynamic key exchange. The Security Server authenticates using a shared secret which is used as an HMAC-SHA1 key to calculate the keyed hash of messages sent to the Gateway during dynamic key exchange. The Security Server IP address and password are configured on the Gateway by the Crypto Officer. Only one Security Server is supported.

The Security Server performs following services:

- a) Authenticate wireless clients for the Gateway
- b) Perform a DH key exchange with the Gateway to negotiate an AES key
- c) Send unicast key to the Gateway encrypted with the AES key negotiated using a DH key exchange

2.1.2. Authentication Mechanisms and Strength

The following table summarizes the four roles and the type of authentication supported for each role:

Role	Type of Authentication	Authentication Data
Crypto Officer	Role-based	Userid and password
Administrator	Role-based	Userid and password for Web management. HMAC-SHA-1 key for SNMP.
User	Role-based	Static Key (TDES or AES)
Security Server	Role-based	HMAC-SHA-1 (Shared secret)

The following table identifies the strength of authentication for each authentication mechanism supported:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 6 characters => $72^6 = 1.39E11$
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)

HMAC-SHA-1 shared secret (Security Server)	Minimum 6 characters => $72^6 = 1.39E11$
HMAC-SHA-1 SNMP key	Minimum 8 characters => $72^8 = 7.22E14$

3. Secure Operation and Security Rules

In order to operate the 3e-DMG securely, each operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules detailed in this section.

3.1. Security Rules

The following 3e-DMG security rules must be followed by the operator in order to ensure secure operation:

1. Every operator (Crypto Officer or Administrator) has a user-id on the 3e-DMG. No operator will violate trust by sharing his/her password associated with the user-id with any other operator or entity.
2. The Crypto Officer will not share any key, or SRDI used by the 3e-DMG with any other operator or entity.
3. The Crypto Officer will not share any MAC address filtering information used by the 3e-DMG with any other operator or entity.
4. The operators will explicitly logoff by closing all secure browser sessions established with the 3e-DMG.
5. The operator will disable browser cookies and password storing mechanisms on the browser used for web configuration of the Gateway.
6. The Crypto officer is responsible for inspecting the tamper evident seals on a daily basis. A compromised tape reveals message "OPENED" with visible red dots. Other signs of tamper include wrinkles, tears and marks on or around the label.
7. The Crypto Officer should change the default password when configuring the Gateway for the first time. The default password should not be used.

3.2. Physical Security Rules

The following section contains detailed instructions to the Crypto Officer concerning where and how to apply the tamper evident seals to the Gateway enclosure, in order to provide physical security for FIPS 140-2 level 2 requirements.

Security seals were added to the back plate side of enclosure on flat of all antenna connectors. A 1/2" 440 Pan head screw replaces the lower right screw on each circular connector. Then two 440 kept nuts were added and tightened together with washers facing each other 1/32" from the pem. This prevents the screws from being removed and thus entry cannot be obtained without removing the security labels. This description only applies to the 525A and the 525N. The 519 details are provided below. The physical security instructions below are detailed for the 525A, 525N, and 519 separately.

Tools:

Wire Cutters (wire seal removal)

Materials:

Gateway, 3eTI – Quantity: 1

Seal, Tape, Tamper-evident – Quantity: 6 for 525A and 525N; 2 for 519

Isopropyl Alcohol Swab

3M Adhesive Remover (citrus or petroleum based solvent)

Installation – Tamper-evident tape

1. Locate on Gateway the placement locations of tamper-evident tape seals. (3 locations as shown in Figure 1 and 2 for the 3e-525A and in Figure 3 and 4 for the 3e-525N and 2 locations as shown in Figure 5 and 6 for the 3e-519).
2. Thoroughly clean area where tamper-evident tape seal is to be applied with isopropyl alcohol swab. Area must be clean of all oils and foreign matter (dirt, grime, etc.)
3. Record tracking number from tamper-evident tape seal.
4. Apply seal to locations on the 3e-525A Gateway as shown in Figures 1 and 2, ones on the 3e-525N Gateway as shown in Figures 3 and 4 and ones on the 3e-519 Gateway as shown in Figure 5 and 6. It is important to ensure that the seal has equal contact area with both top and bottom housings.
5. After application of seals to the Gateway, apply pressure to verify that adequate adhesion has taken place.

Removal – Tamper-evident tape

1. Locate on Gateway locations of tamper-evident tape seals. (3 locations as shown in Figures 1 and 2 for the 3e-525A, 3 locations as shown in Figures 3 and 4 and 2 locations as shown in Figure 5 and 6 for the 3e-519)
2. Record tracking numbers from existing tamper-evident tape seal and verify physical condition as not tampered or destroyed after installation.
3. Cut tape along seam of Gateway to allow opening of enclosure.
4. Remove nut and washer from antenna connectors.
5. Using 3M adhesive remover or equivalent, remove residual tamper-evident seal tape. (Three locations as shown in Figures 1 and 2 for the 3e-525A, in Figure 3 and 4 for the 3e-525N and two locations as shown in Figures 5 and 6 for the 3e-519)

This picture shows the physical interface side of 3e-525A Gateway enclosure with tamper-evident seal.

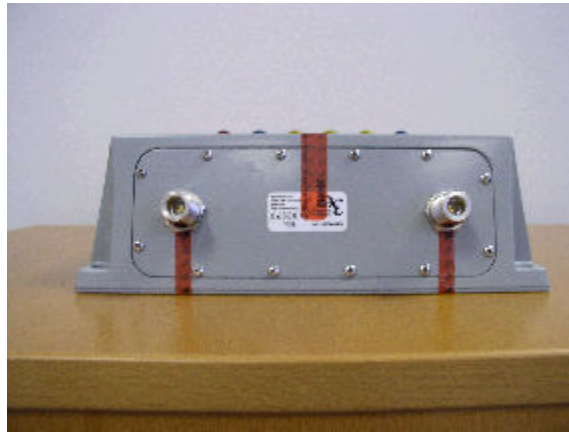


Figure 1

End-view of 3e-525A Gateway showing WLAN antenna port and tamper-evident seal:



Figure 2

This picture shows the physical interface side of 3e-525N Gateway enclosure with tamper-evident seal.



Figure 3

End-view of 3e-525N Gateway showing WLAN antenna port and tamper-evident seal:



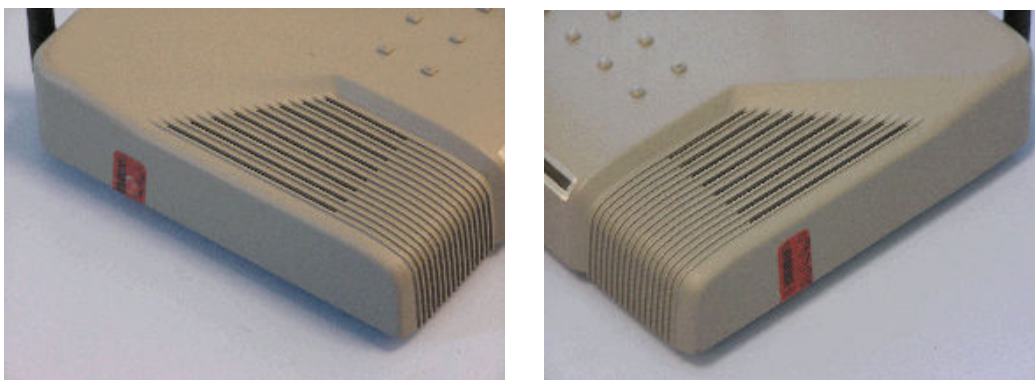
Figure 4

This picture shows the physical interface side of 3e-519 Gateway enclosure with tamper-evident seal.



Figure 5

Side-view of 3e-519 Gateway showing WLAN antenna port and tamper-evident seal:

**Figure 6**

3.3. Secure Operation Initialization

The following procedures describe the way to configure the module in FIPS mode.

There is a default Crypto Officer password, which can be used to access the configuration pages using HTTPS from any browser. The LAN port by default is configured with the IP address 192.168.15.1.

Using any browser, open the page <https://192.168.15.1> to access the Gateway configuration. The main configuration page is shown below:

3eTI Gateway Configuration - Microsoft Internet Explorer

Address: https://192.168.15.1/cgi-bin/sgateway?PG=0

3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
 Security Mode: FIPS 140-2
 Username: CryptoOfficer
 Role: Crypto Officer
 Host Name: default (192.168.254.254)

System Configuration -> General

Version: 3eTI DMG Wireless Access Point - Version 3.0

Host Name:

Domain Name:

System Date: 11/30/1999 (Month Day Year)

System Time: 0:01 : (Hour:Minute)

System Configuration

- General
- WAN
- LAN
- Operating Mode

Wireless Configuration

- General
- Security
- MAC Address Filtering
- Bridging
- Bridging Encryption
- Rogue AP Detection
- Advanced

Services Settings

- DHCP Server
- Subnet Roaming
- SNMP Agent
- Misc Service

User Management

- List All Users
- Add New User
- User Password Policy

Monitoring/Reports

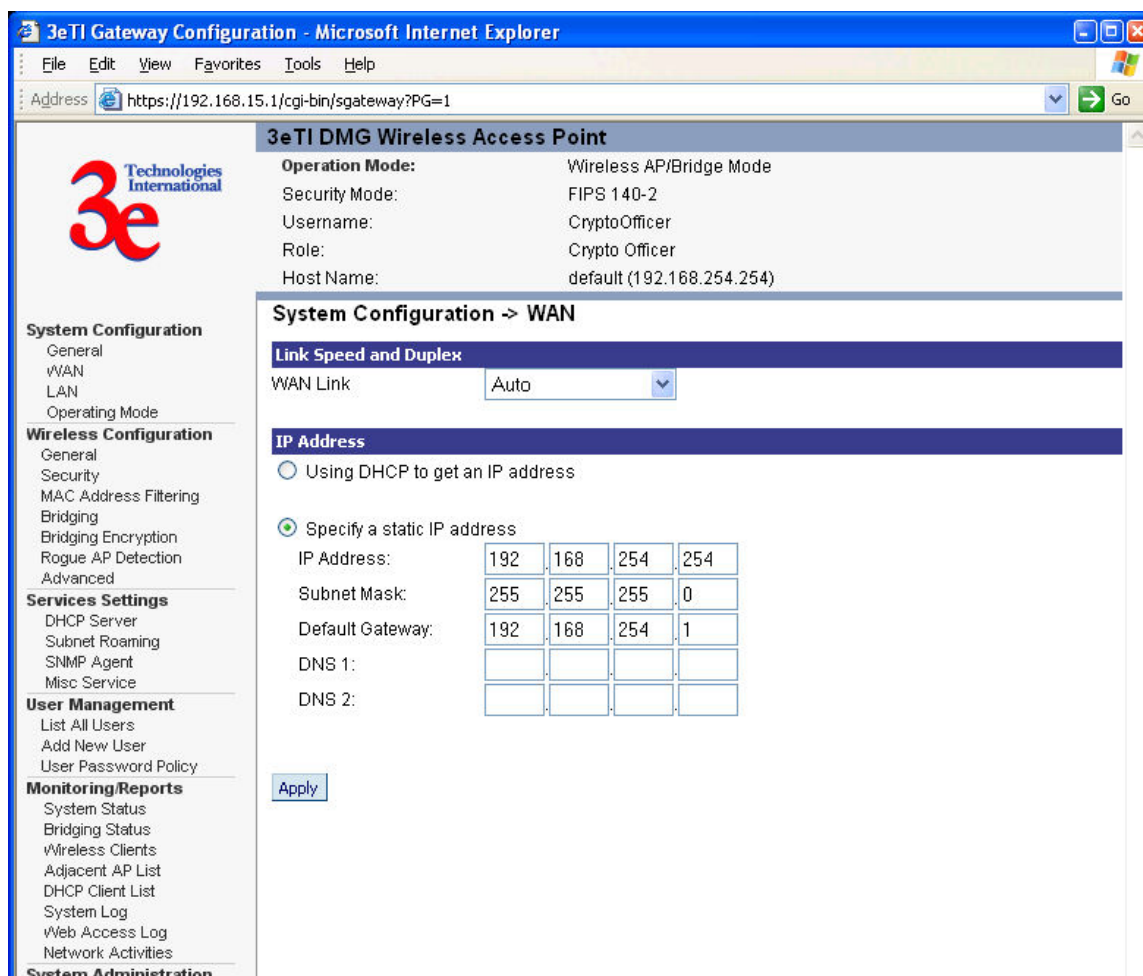
- System Status
- Bridging Status
- Wireless Clients
- Adjacent AP List
- DHCP Client List
- System Log
- Web Access Log
- Network Activities

System Administration

3.3.1. System Configuration

3.3.1.1. WAN Configuration

The IP address of the WAN interface can be configured with Static IP address or by using DHCP to obtain an IP address.



3eTI Gateway Configuration - Microsoft Internet Explorer

Address: <https://192.168.15.1/cgi-bin/sgateway?PG=1> Go

3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
 Security Mode: FIPS 140-2
 Username: CryptoOfficer
 Role: Crypto Officer
 Host Name: default (192.168.254.254)

System Configuration

- General
- WAN
- LAN
- Operating Mode

Wireless Configuration

- General
- Security
- MAC Address Filtering
- Bridging
- Bridging Encryption
- Rogue AP Detection
- Advanced

Services Settings

- DHCP Server
- Subnet Roaming
- SNMP Agent
- Misc Service

User Management

- List All Users
- Add New User
- User Password Policy

Monitoring/Reports

- System Status
- Bridging Status
- Wireless Clients
- Adjacent AP List
- DHCP Client List
- System Log
- Web Access Log
- Network Activities

System Administration

System Configuration -> WAN

Link Speed and Duplex

WAN Link: Auto

IP Address

☐ Using DHCP to get an IP address

☒ Specify a static IP address

IP Address:

192	168	254	254
-----	-----	-----	-----

Subnet Mask:

255	255	255	0
-----	-----	-----	---

Default Gateway:

192	168	254	1
-----	-----	-----	---

DNS 1:

--	--	--	--

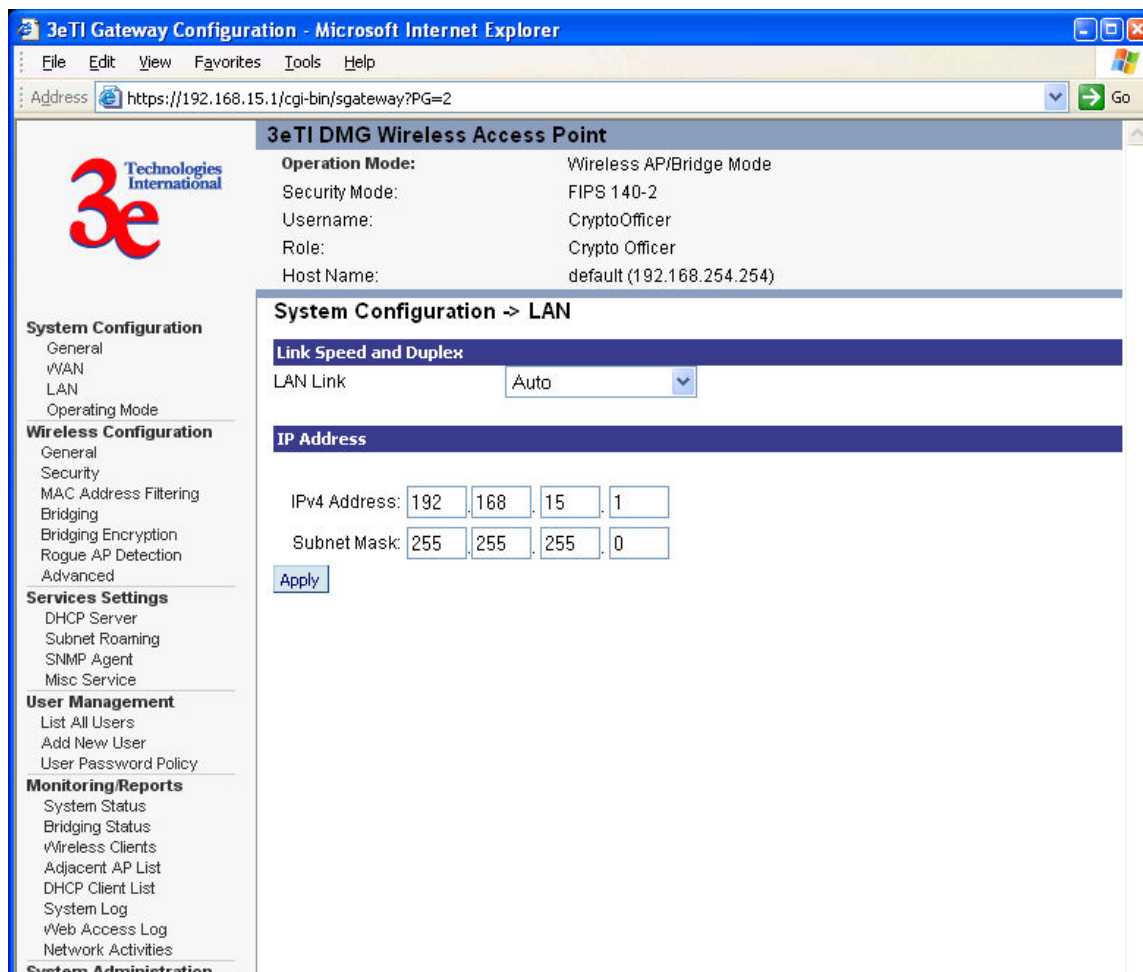
DNS 2:

--	--	--	--

Apply

3.3.1.2. LAN Configuration

The IP address of the LAN interface can be configured with a static IP address, by using the link under System Configuration.



3eTI Gateway Configuration - Microsoft Internet Explorer

Address: <https://192.168.15.1/cgi-bin/sgateway?PG=2> Go

3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer
Host Name: default (192.168.254.254)

System Configuration -> LAN

Link Speed and Duplex

LAN Link: Auto

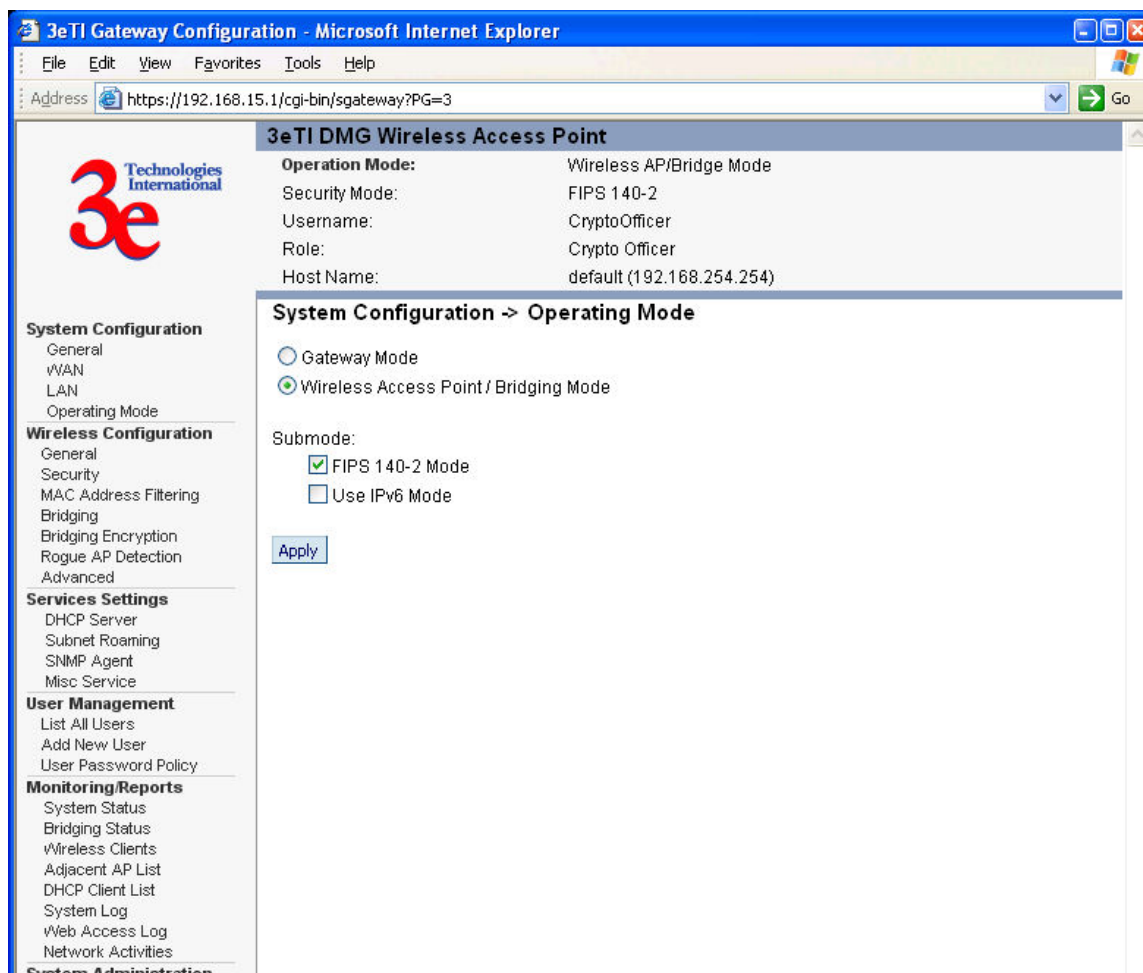
IP Address

IPv4 Address: 192 . 168 . 15 . 1
 Subnet Mask: 255 . 255 . 255 . 0

Apply

3.3.1.3. Operating Mode

The gateway can be configured in *Gateway Mode – non-FIPS*, *Gateway Mode – FIPS*, *Wireless Access Point/Bridging Mode – FIPS* and *Wireless Access Point/Bridging Mode-non-FIPS* by using the Operating Mode link. It is important to note that the unit will be reset to factory default when the Operating mode is changed. To put the module in FIPS mode one of the above FIPS modes must be selected.



3eTI Gateway Configuration - Microsoft Internet Explorer

Address: https://192.168.15.1/cgi-bin/sgateway?PG=3

3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer
Host Name: default (192.168.254.254)

System Configuration -> Operating Mode

☐ Gateway Mode
☒ Wireless Access Point / Bridging Mode

Submode:
☒ FIPS 140-2 Mode
☐ Use IPv6 Mode

System Configuration
 General
 WAN
 LAN
 Operating Mode

Wireless Configuration
 General
 Security
 MAC Address Filtering
 Bridging
 Bridging Encryption
 Rogue AP Detection
 Advanced

Services Settings
 DHCP Server
 Subnet Roaming
 SNMP Agent
 Misc Service

User Management
 List All Users
 Add New User
 User Password Policy

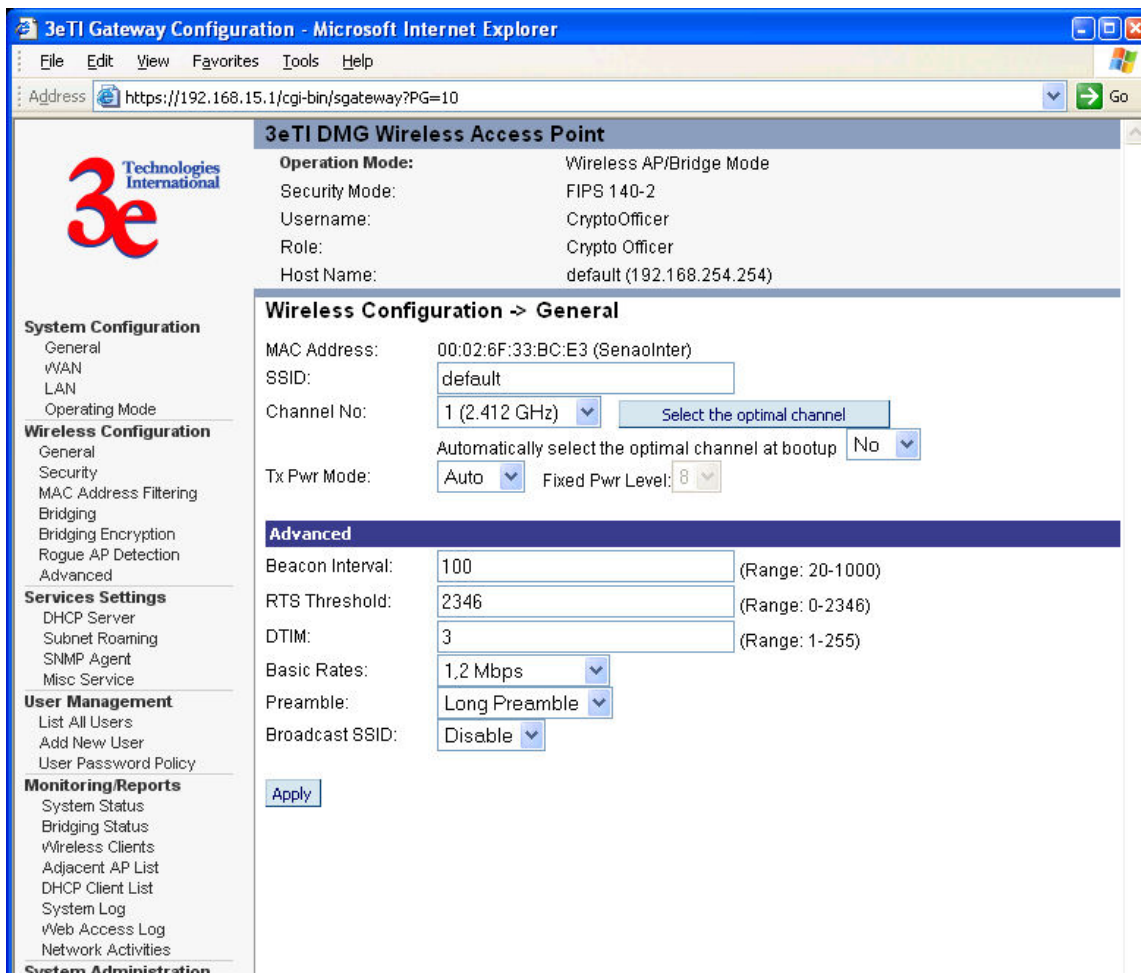
Monitoring/Reports
 System Status
 Bridging Status
 Wireless Clients
 Adjacent AP List
 DHCP Client List
 System Log
 Web Access Log
 Network Activities

System Administration

3.3.2. Wireless Configuration

3.3.2.1. General

This screen can be used to configure the access point's wireless settings like SSID, channel and transmit power.



3eTI Gateway Configuration - Microsoft Internet Explorer

Address: <https://192.168.15.1/cgi-bin/sgateway?PG=10> Go

3e Technologies International

System Configuration

- General
- WAN
- LAN
- Operating Mode

Wireless Configuration

- General
- Security
- MAC Address Filtering
- Bridging
- Bridging Encryption
- Rogue AP Detection
- Advanced

Services Settings

- DHCP Server
- Subnet Roaming
- SNMP Agent
- Misc Service

User Management

- List All Users
- Add New User
- User Password Policy

Monitoring/Reports

- System Status
- Bridging Status
- Wireless Clients
- Adjacent AP List
- DHCP Client List
- System Log
- Web Access Log
- Network Activities

System Administration

3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode

Security Mode: FIPS 140-2

Username: CryptoOfficer

Role: Crypto Officer

Host Name: default (192.168.254.254)

Wireless Configuration -> General

MAC Address: 00:02:6F:33:BC:E3 (Senaolnter)

SSID: default

Channel No: 1 (2.412 GHz) [Select the optimal channel](#)

Automatically select the optimal channel at bootup: No

Tx Pwr Mode: Auto **Fixed Pwr Level:** 8

Advanced

Beacon Interval: 100 (Range: 20-1000)

RTS Threshold: 2346 (Range: 0-2346)

DTIM: 3 (Range: 1-255)

Basic Rates: 1,2 Mbps

Preamble: Long Preamble

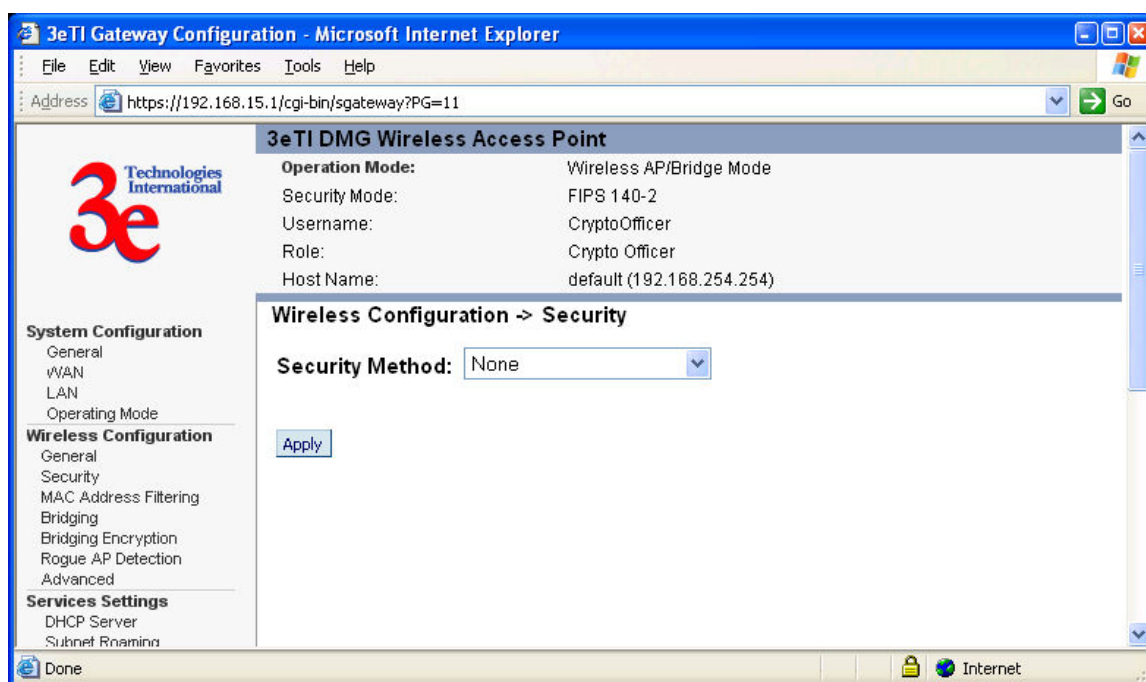
Broadcast SSID: Disable

[Apply](#)

3.3.2.2. Encryption

No Data Encryption

Factory default sets the encryption to “*No Data Encryption*”. This results in all wireless traffic being sent in plaintext form.



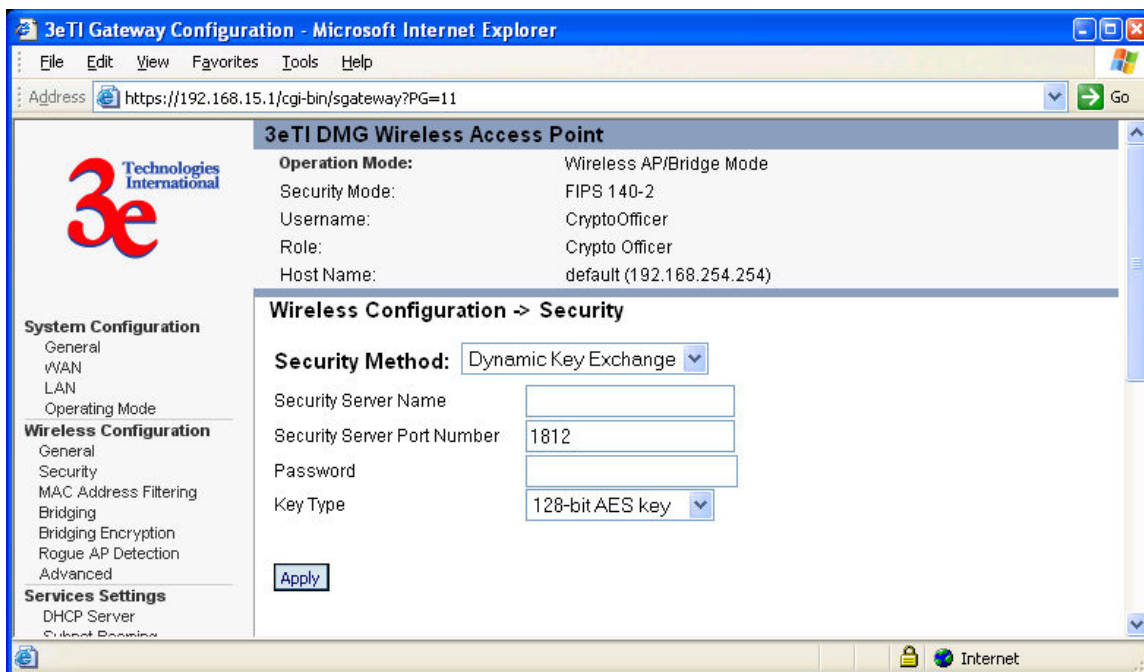
Dynamic Key Management

Using this configuration, the Crypto Officer can set per session keys dynamically.

The configuration entails the following:

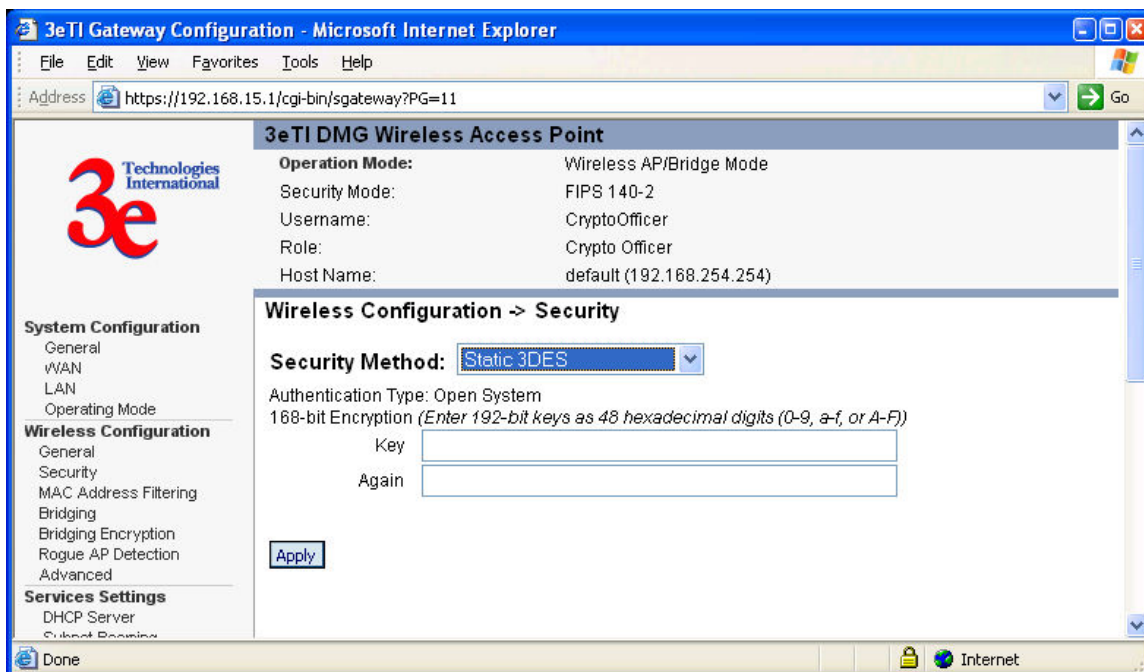
Gateway Configuration:

- Configure the IP address of the security server in the *Security Server IP Address* box.
- Configure the port number of the security server.
- Configure the Security Server password.
- Select the type of key. The options available are:
 - AES 128-bit key
 - AES 192-bit key
 - AES 256-bit key
 - 3DES key



Static 3DES Key

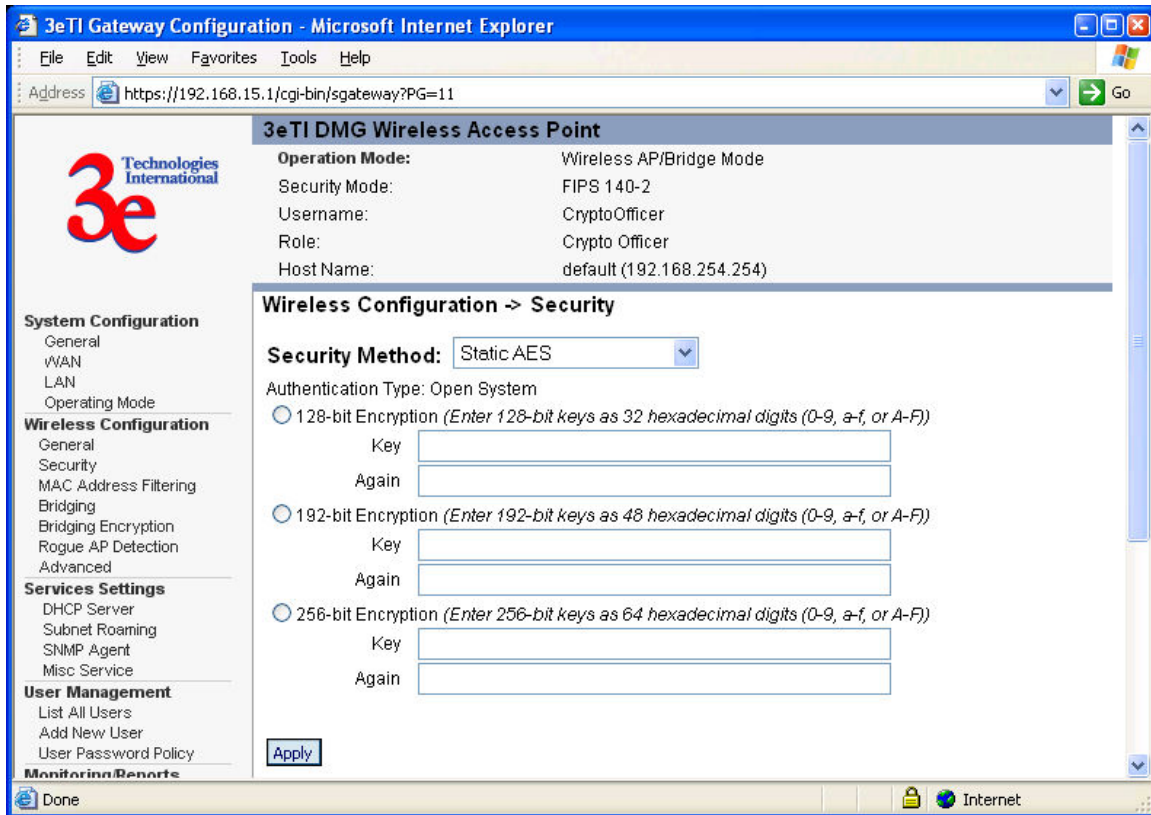
The Crypto Officer can configure the AP to use static 3DES key (192-bit).



Static AES Key

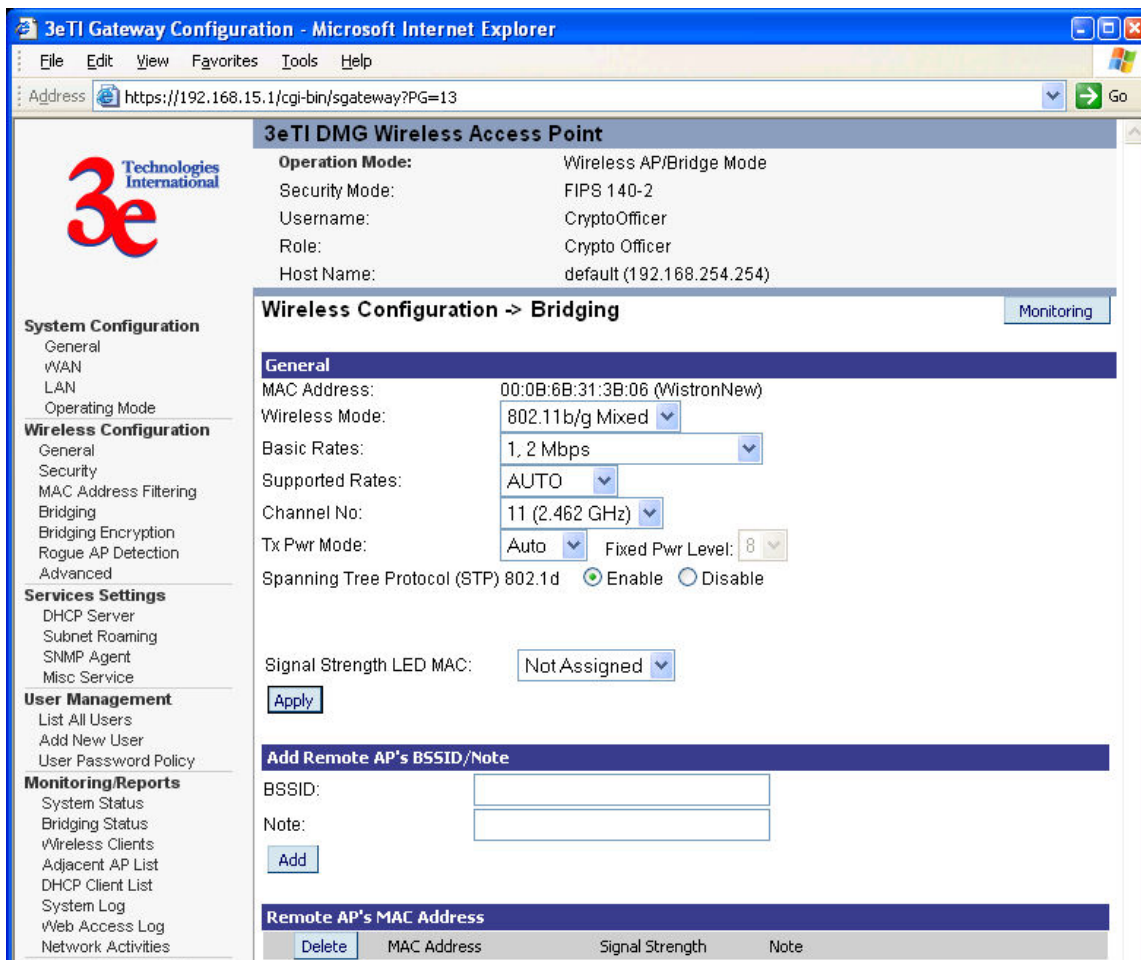
The Crypto Officer can configure the AP to use static AES keys. The following AES keys can be configured:

- AES 128-bit key
- AES 192-bit key
- AES 256-bit key



3.3.2.3. Bridging

This screen is used to configure the remote bridging devices. The MAC address of the remote bridge is needed to allow the two bridges to communicate.



3eTI Gateway Configuration - Microsoft Internet Explorer

Address: <https://192.168.15.1/cgi-bin/sgateway?PG=13>

3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer
Host Name: default (192.168.254.254)

System Configuration
 General
 WAN
 LAN
 Operating Mode

Wireless Configuration
 General
 Security
 MAC Address Filtering
 Bridging
 Bridging Encryption
 Rogue AP Detection
 Advanced

Services Settings
 DHCP Server
 Subnet Roaming
 SNMP Agent
 Misc Service

User Management
 List All Users
 Add New User
 User Password Policy

Monitoring/Reports
 System Status
 Bridging Status
 Wireless Clients
 Adjacent AP List
 DHCP Client List
 System Log
 Web Access Log
 Network Activities

Wireless Configuration -> Bridging Monitoring

General
MAC Address: 00:0B:6B:31:3B:06 (WistronNew)
Wireless Mode: 802.11b/g Mixed
Basic Rates: 1, 2 Mbps
Supported Rates: AUTO
Channel No: 11 (2.462 GHz)
Tx Pwr Mode: Auto Fixed Pwr Level: 8
Spanning Tree Protocol (STP) 802.1d: ☒ Enable ☐ Disable

Signal Strength LED MAC: Not Assigned

Apply

Add Remote AP's BSSID/Note
BSSID:
Note:
Add

Remote AP's MAC Address

Delete	MAC Address	Signal Strength	Note
--------	-------------	-----------------	------

3.3.2.4. Bridging Encryption

No Data Encryption

Factory default sets the encryption to “*No Data Encryption*”. This results in all bridging traffic being sent in plaintext form.

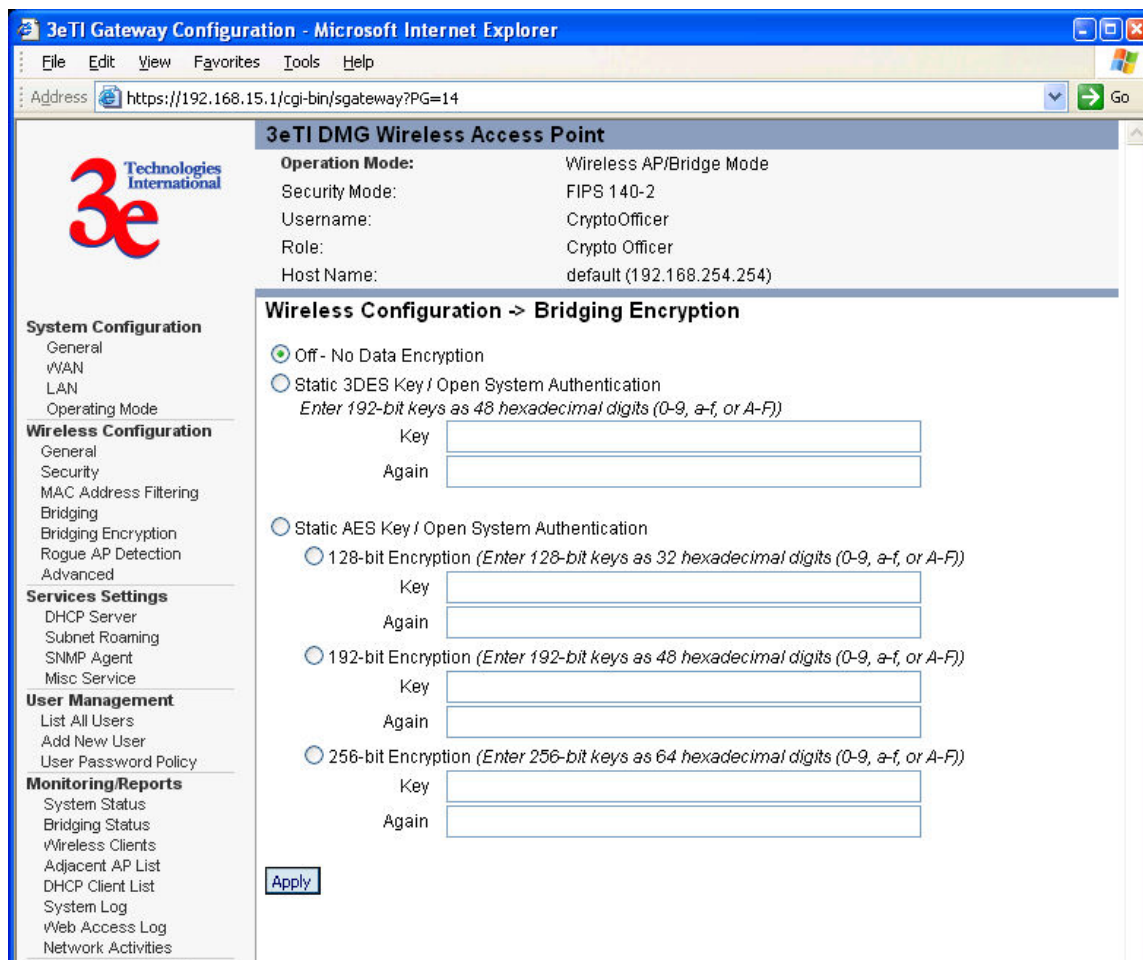
Static 3DES Key

The Crypto Officer can configure the bridge to use static 3DES key (192-bit).

Static AES Key

The Crypto Officer can configure the bridge to use AES keys. The following AES keys can be configured:

- AES 128-bit key
- AES 192-bit key
- AES 256-bit key



The screenshot shows the '3eTI Gateway Configuration - Microsoft Internet Explorer' window. The address bar displays 'https://192.168.15.1/cgi-bin/sgateway?PG=14'. The main content area is titled '3eTI DMG Wireless Access Point' and shows the following configuration details:

- Operation Mode: Wireless AP/Bridge Mode
- Security Mode: FIPS 140-2
- Username: CryptoOfficer
- Role: Crypto Officer
- Host Name: default (192.168.254.254)

The 'Wireless Configuration -> Bridging Encryption' section is active, showing the following options:

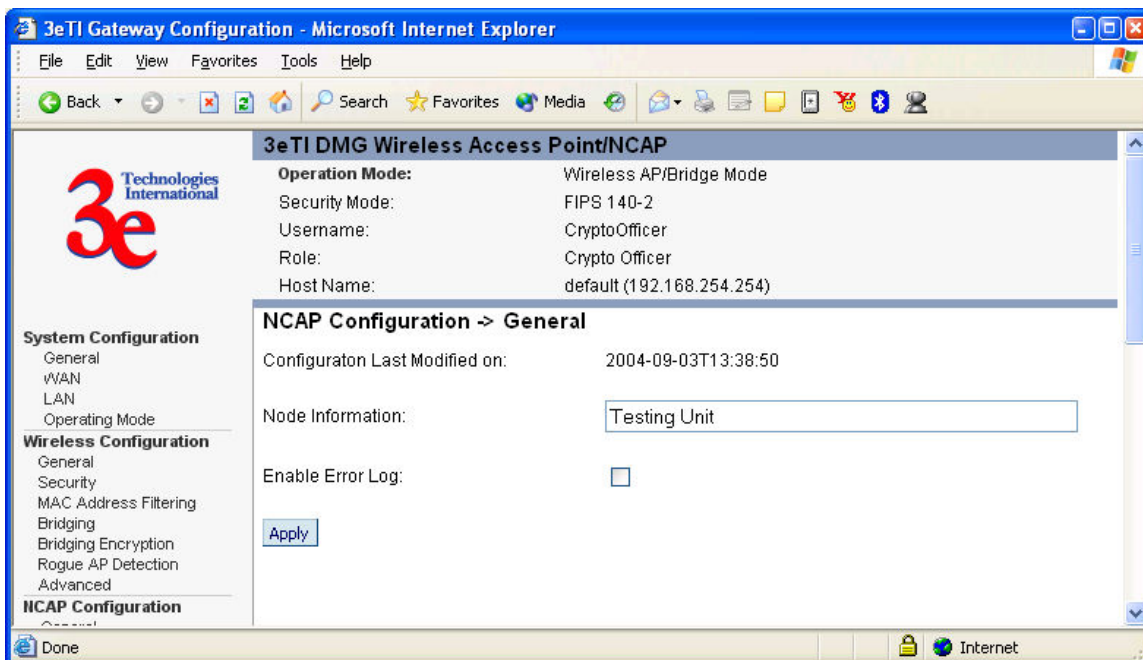
- ☒ Off - No Data Encryption
- ☐ Static 3DES Key / Open System Authentication
 - Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F)
 - Key:
 - Again:
- ☐ Static AES Key / Open System Authentication
 - ☐ 128-bit Encryption (Enter 128-bit keys as 32 hexadecimal digits (0-9, a-f, or A-F))
 - Key:
 - Again:
 - ☐ 192-bit Encryption (Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F))
 - Key:
 - Again:
 - ☐ 256-bit Encryption (Enter 256-bit keys as 64 hexadecimal digits (0-9, a-f, or A-F))
 - Key:
 - Again:

An 'Apply' button is located at the bottom left of the configuration area.

3.3.3. NCAP Configuration (for 3e-525N only)

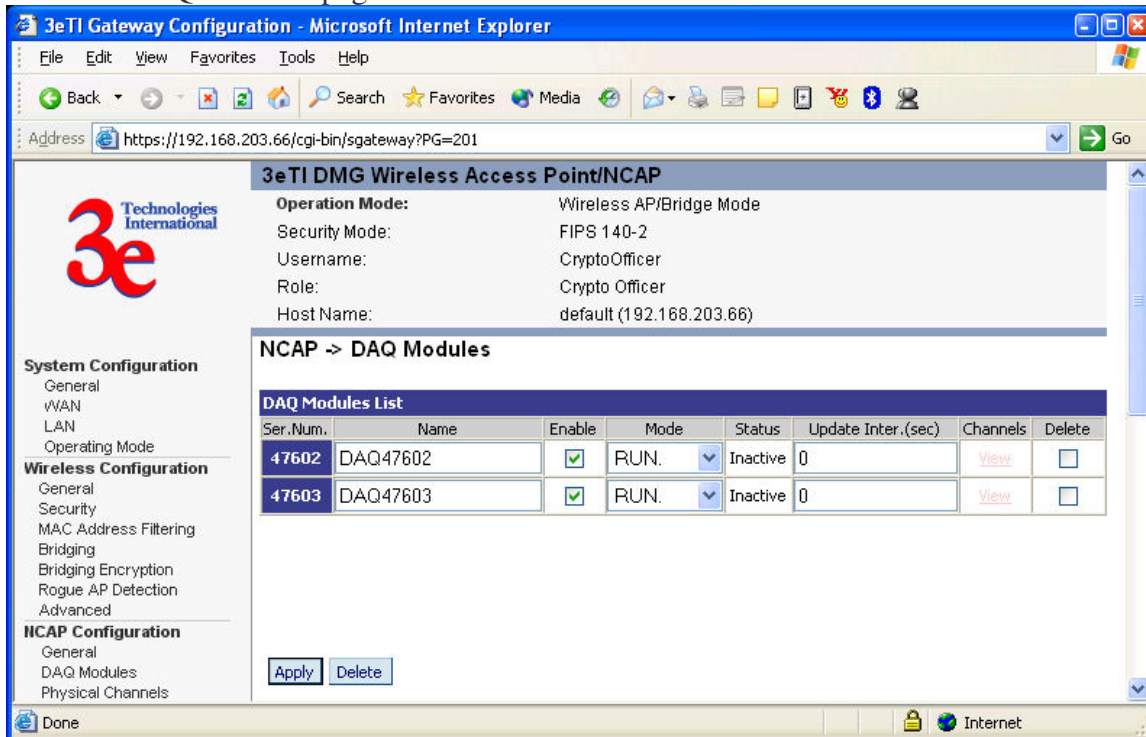
3.3.3.1. General

The NCAP general information which includes “Configuration last modified on”, “Node information” and “Enable error log”.



3.3.3.2. DAQ Modules

NCAP system detects new DAQ box, a corresponding entry for the new DAQ box will be written into the system configuration file. The DAQ information will show up on the NCAP—DAQ Modules page.



3eTI Gateway Configuration - Microsoft Internet Explorer

Address: <https://192.168.203.66/cgi-bin/sgateway?PG=201>

3eTI DMG Wireless Access Point/NCAP

Operation Mode: Wireless AP/Bridge Mode
 Security Mode: FIPS 140-2
 Username: CryptoOfficer
 Role: Crypto Officer
 Host Name: default (192.168.203.66)

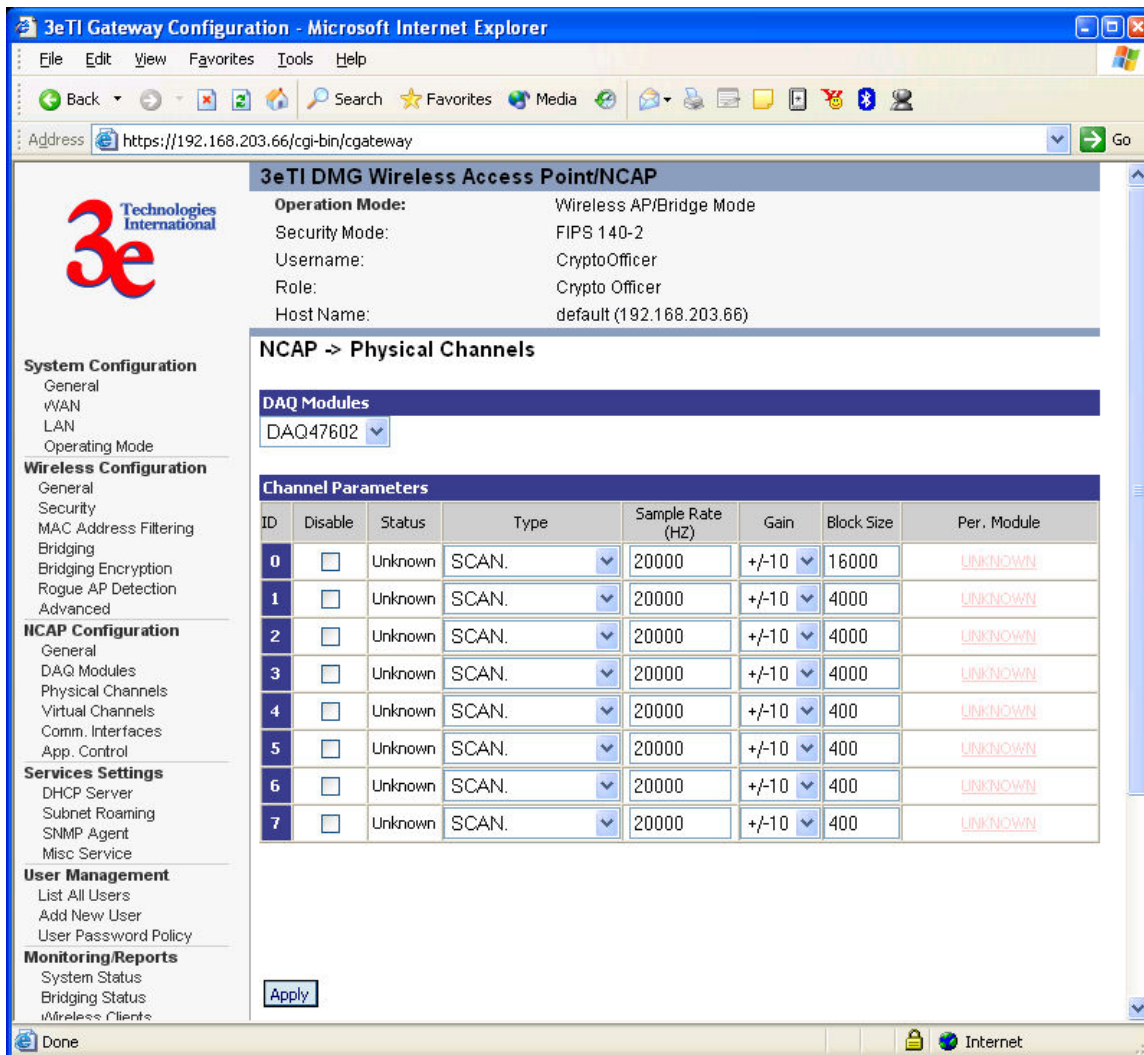
NCAP -> DAQ Modules

Ser.Num.	Name	Enable	Mode	Status	Update Inter.(sec)	Channels	Delete
47602	DAQ47602	<input checked="" type="checkbox"/>	RUN.	Inactive	0	View	<input type="checkbox"/>
47603	DAQ47603	<input checked="" type="checkbox"/>	RUN.	Inactive	0	View	<input type="checkbox"/>

[Apply](#) [Delete](#)

3.3.3.3. Physical Channels

The physical channel page enable you to set the individual channel parameters, which includes channel gain, sample frequency, sample size, enabling or disabling particular channel, etc.



The screenshot shows the 3eTI Gateway Configuration web interface in Microsoft Internet Explorer. The address bar shows the URL: `https://192.168.203.66/cgi-bin/cgateway`. The page title is "3eTI DMG Wireless Access Point/NCAP".

System Configuration

- General
- WAN
- LAN
- Operating Mode

Wireless Configuration

- General
- Security
- MAC Address Filtering
- Bridging
- Bridging Encryption
- Rogue AP Detection
- Advanced

NCAP Configuration

- General
- DAQ Modules
- Physical Channels
- Virtual Channels
- Comm. Interfaces
- App. Control

Services Settings

- DHCP Server
- Subnet Roaming
- SNMP Agent
- Misc Service

User Management

- List All Users
- Add New User
- User Password Policy

Monitoring/Reports

- System Status
- Bridging Status
- Wireless Clients

3eTI DMG Wireless Access Point/NCAP

Operation Mode: Wireless AP/Bridge Mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer
Host Name: default (192.168.203.66)

NCAP -> Physical Channels

DAQ Modules

DAQ47602

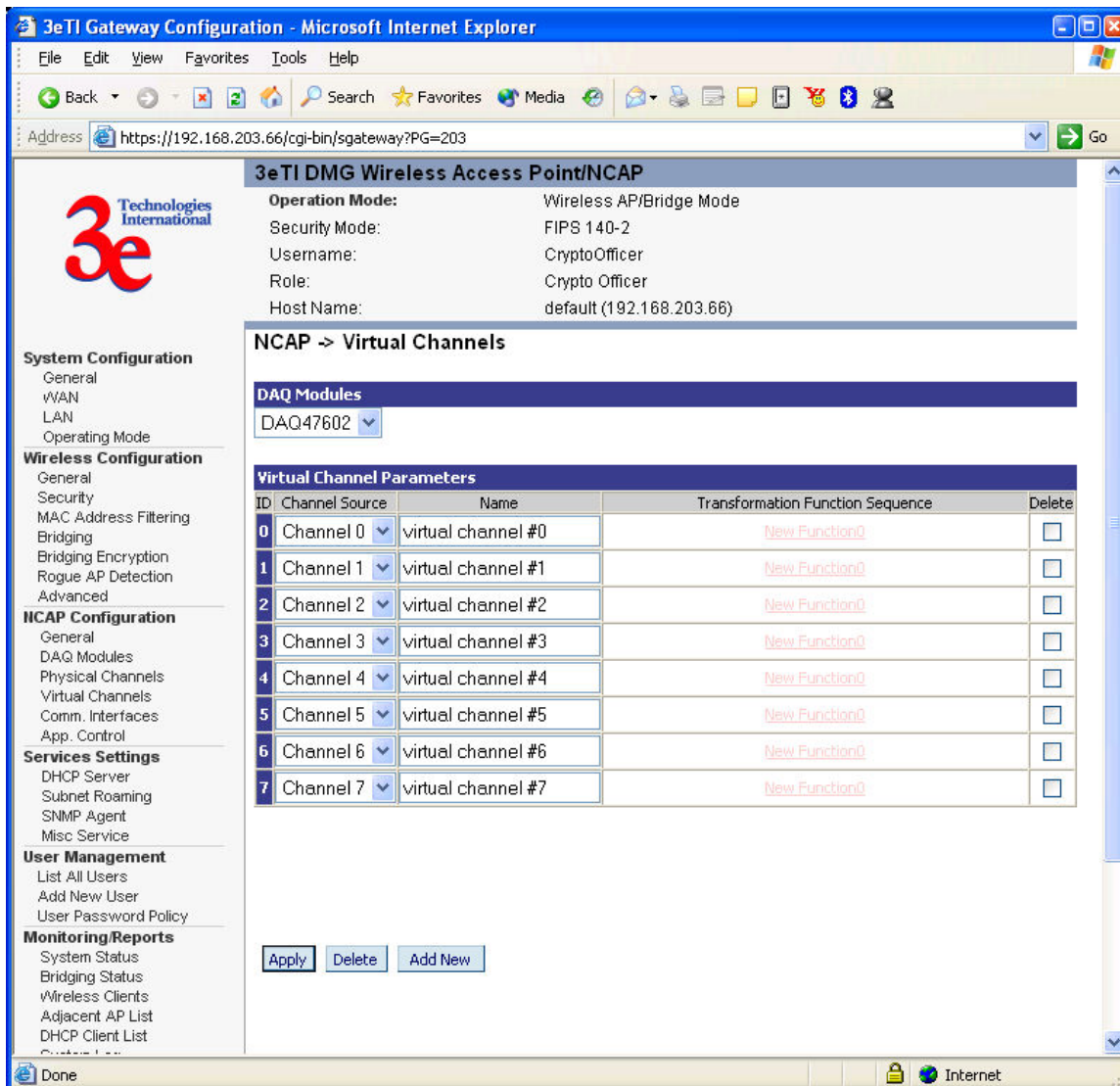
Channel Parameters

ID	Disable	Status	Type	Sample Rate (HZ)	Gain	Block Size	Per. Module
0	<input type="checkbox"/>	Unknown	SCAN.	20000	+/-10	16000	UNKNOWN
1	<input type="checkbox"/>	Unknown	SCAN.	20000	+/-10	4000	UNKNOWN
2	<input type="checkbox"/>	Unknown	SCAN.	20000	+/-10	4000	UNKNOWN
3	<input type="checkbox"/>	Unknown	SCAN.	20000	+/-10	4000	UNKNOWN
4	<input type="checkbox"/>	Unknown	SCAN.	20000	+/-10	400	UNKNOWN
5	<input type="checkbox"/>	Unknown	SCAN.	20000	+/-10	400	UNKNOWN
6	<input type="checkbox"/>	Unknown	SCAN.	20000	+/-10	400	UNKNOWN
7	<input type="checkbox"/>	Unknown	SCAN.	20000	+/-10	400	UNKNOWN

Apply

3.3.3.4. Virtual Channels

Once a new DAQ module is detected, the NCAP application will automatically create 8 virtual channels for each physical channel. You will need to configure the virtual channels transformation sequence according to your sensors.



The screenshot shows the 3eTI Gateway Configuration web interface in Microsoft Internet Explorer. The browser address bar shows <https://192.168.203.66/cgi-bin/sgateway?PG=203>. The page title is "3eTI DMG Wireless Access Point/NCAP".

System Configuration

- General
- WAN
- LAN
- Operating Mode

Wireless Configuration

- General
- Security
- MAC Address Filtering
- Bridging
- Bridging Encryption
- Rogue AP Detection
- Advanced

NCAP Configuration

- General
- DAQ Modules
- Physical Channels
- Virtual Channels
- Comm. Interfaces
- App. Control

Services Settings

- DHCP Server
- Subnet Roaming
- SNMP Agent
- Misc Service

User Management

- List All Users
- Add New User
- User Password Policy

Monitoring/Reports

- System Status
- Bridging Status
- Wireless Clients
- Adjacent AP List
- DHCP Client List

3eTI DMG Wireless Access Point/NCAP

Operation Mode: Wireless AP/Bridge Mode

Security Mode: FIPS 140-2

Username: CryptoOfficer

Role: Crypto Officer

Host Name: default (192.168.203.66)

NCAP -> Virtual Channels

DAQ Modules

DAQ47602

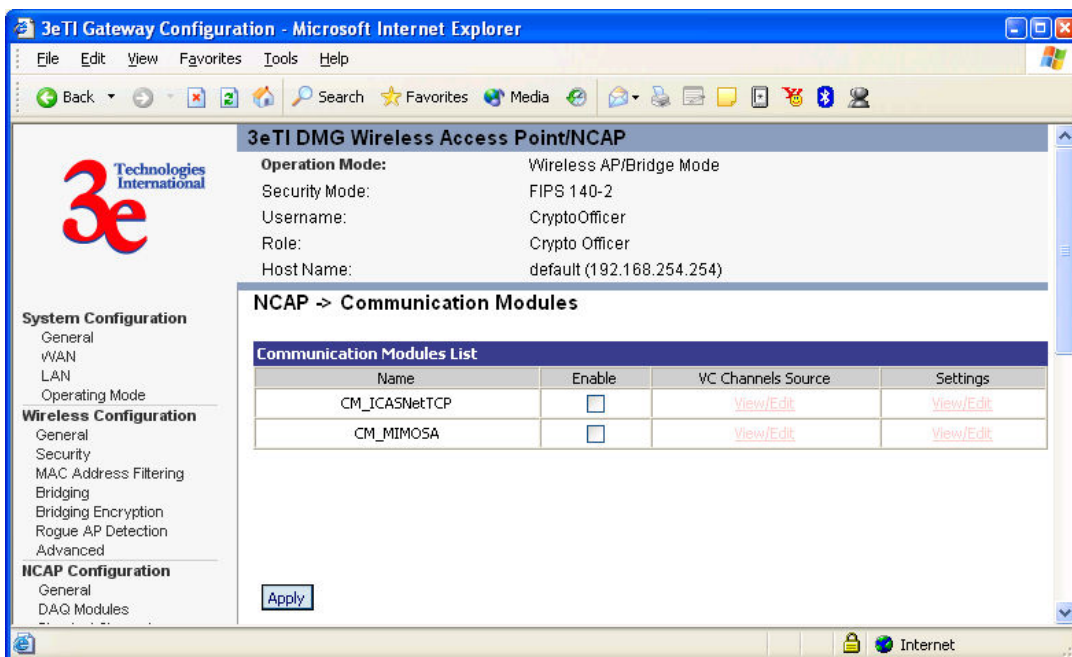
Virtual Channel Parameters

ID	Channel Source	Name	Transformation Function Sequence	Delete
0	Channel 0	virtual channel #0	New Function0	<input type="checkbox"/>
1	Channel 1	virtual channel #1	New Function0	<input type="checkbox"/>
2	Channel 2	virtual channel #2	New Function0	<input type="checkbox"/>
3	Channel 3	virtual channel #3	New Function0	<input type="checkbox"/>
4	Channel 4	virtual channel #4	New Function0	<input type="checkbox"/>
5	Channel 5	virtual channel #5	New Function0	<input type="checkbox"/>
6	Channel 6	virtual channel #6	New Function0	<input type="checkbox"/>
7	Channel 7	virtual channel #7	New Function0	<input type="checkbox"/>

Buttons: Apply, Delete, Add New

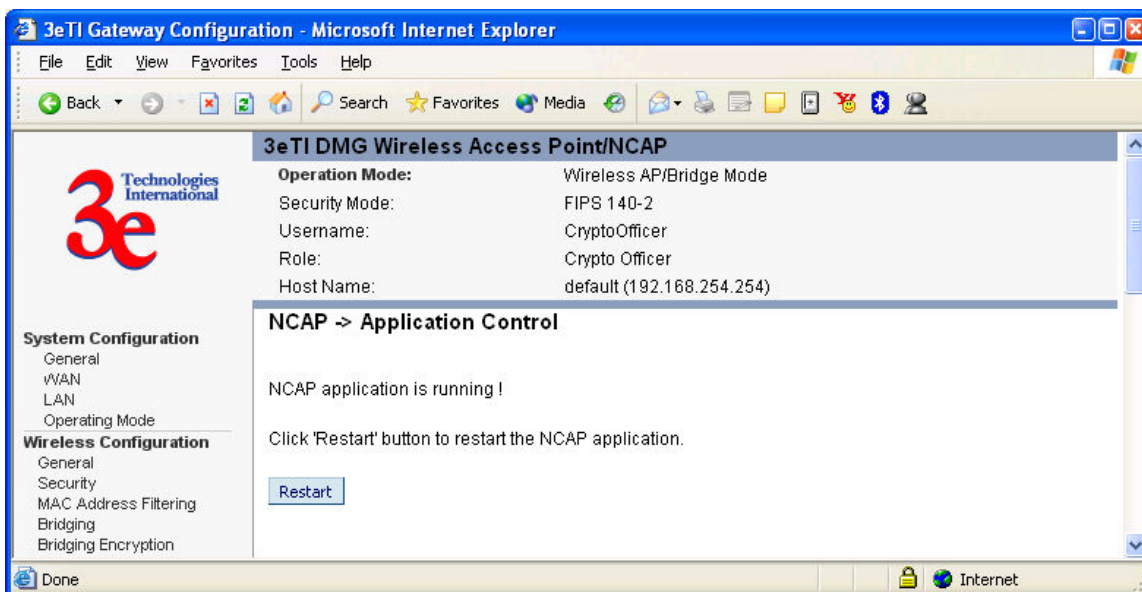
3.3.3.5. Communication Modules

NCAP provides 2 types of communication interfaces: ICASNetTCP and MIMOSA.



3.3.3.6. Application Control

Whenever NCAP configuration has been changed, in order to make the new configuration take effect, user must click on the “Restart” button to restart the NCAP application.

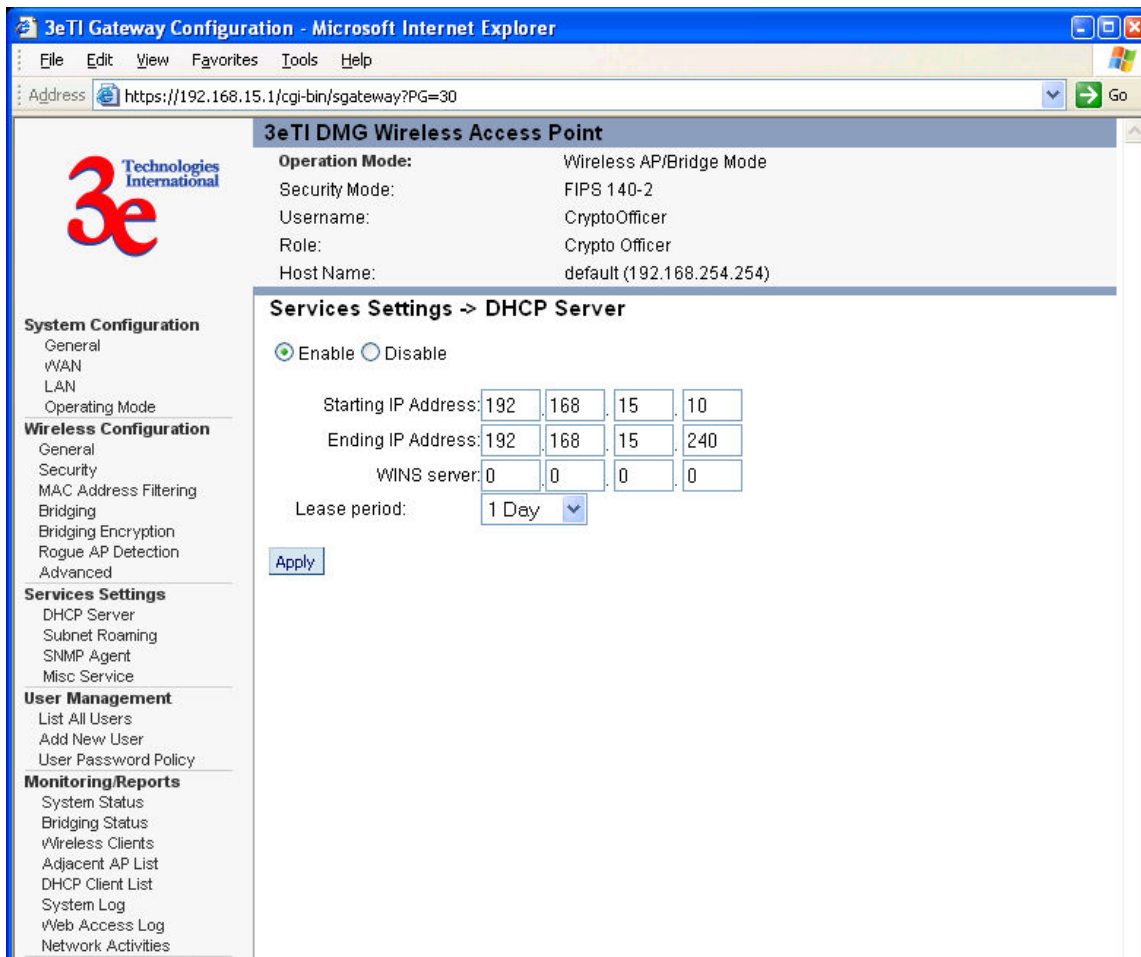


3.3.4. Services Settings

3.3.4.1. DHCP server

Using this link, the DHCP server for the LAN port can be configured.

- The DHCP server can be enabled or disabled.
- The IP address range can be configured.



The screenshot shows the '3eTI Gateway Configuration - Microsoft Internet Explorer' window. The address bar displays 'https://192.168.15.1/cgi-bin/sgateway?PG=30'. The main content area is titled '3eTI DMG Wireless Access Point' and shows the following configuration:

- Operation Mode:** Wireless AP/Bridge Mode
- Security Mode:** FIPS 140-2
- Username:** CryptoOfficer
- Role:** Crypto Officer
- Host Name:** default (192.168.254.254)

The left sidebar contains a navigation menu with the following sections:

- System Configuration**
 - General
 - WAN
 - LAN
 - Operating Mode
- Wireless Configuration**
 - General
 - Security
 - MAC Address Filtering
 - Bridging
 - Bridging Encryption
 - Rogue AP Detection
 - Advanced
- Services Settings**
 - DHCP Server
 - Subnet Roaming
 - SNMP Agent
 - Misc Service
- User Management**
 - List All Users
 - Add New User
 - User Password Policy
- Monitoring/Reports**
 - System Status
 - Bridging Status
 - Wireless Clients
 - Adjacent AP List
 - DHCP Client List
 - System Log
 - Web Access Log
 - Network Activities

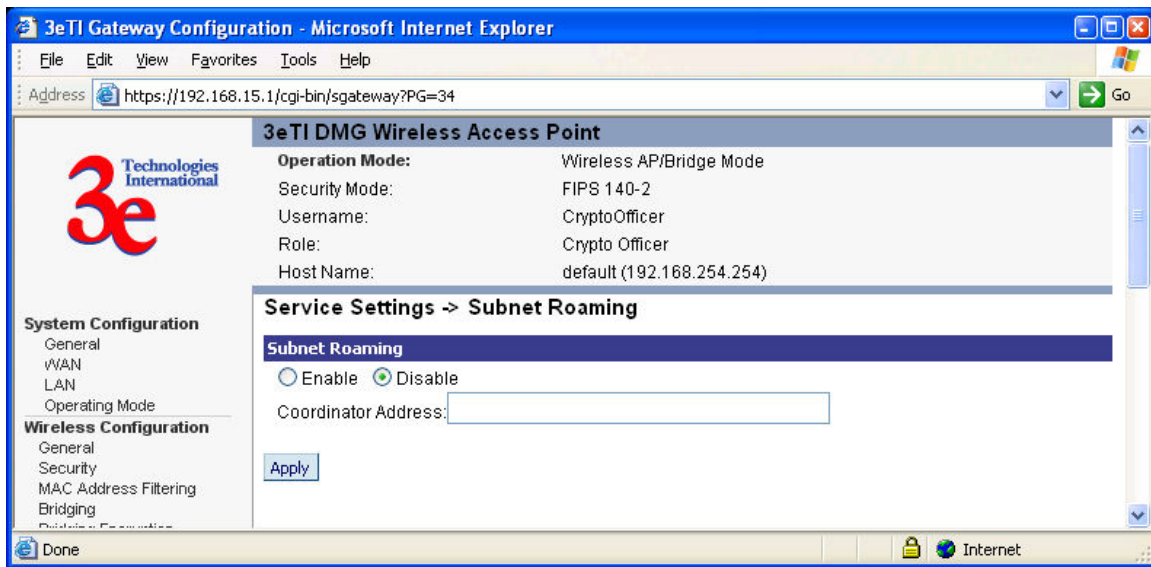
The main content area is titled 'Services Settings -> DHCP Server'. It includes the following settings:

- Enable** (selected) **Disable**
- Starting IP Address:** 192.168.15.10
- Ending IP Address:** 192.168.15.240
- WINS server:** 0.0.0.0
- Lease period:** 1 Day
- Apply** button

3.3.4.2. Subnet Roaming

The subnet roaming service provides the seamless roaming for wireless client among different networks without disconnecting the wireless client.

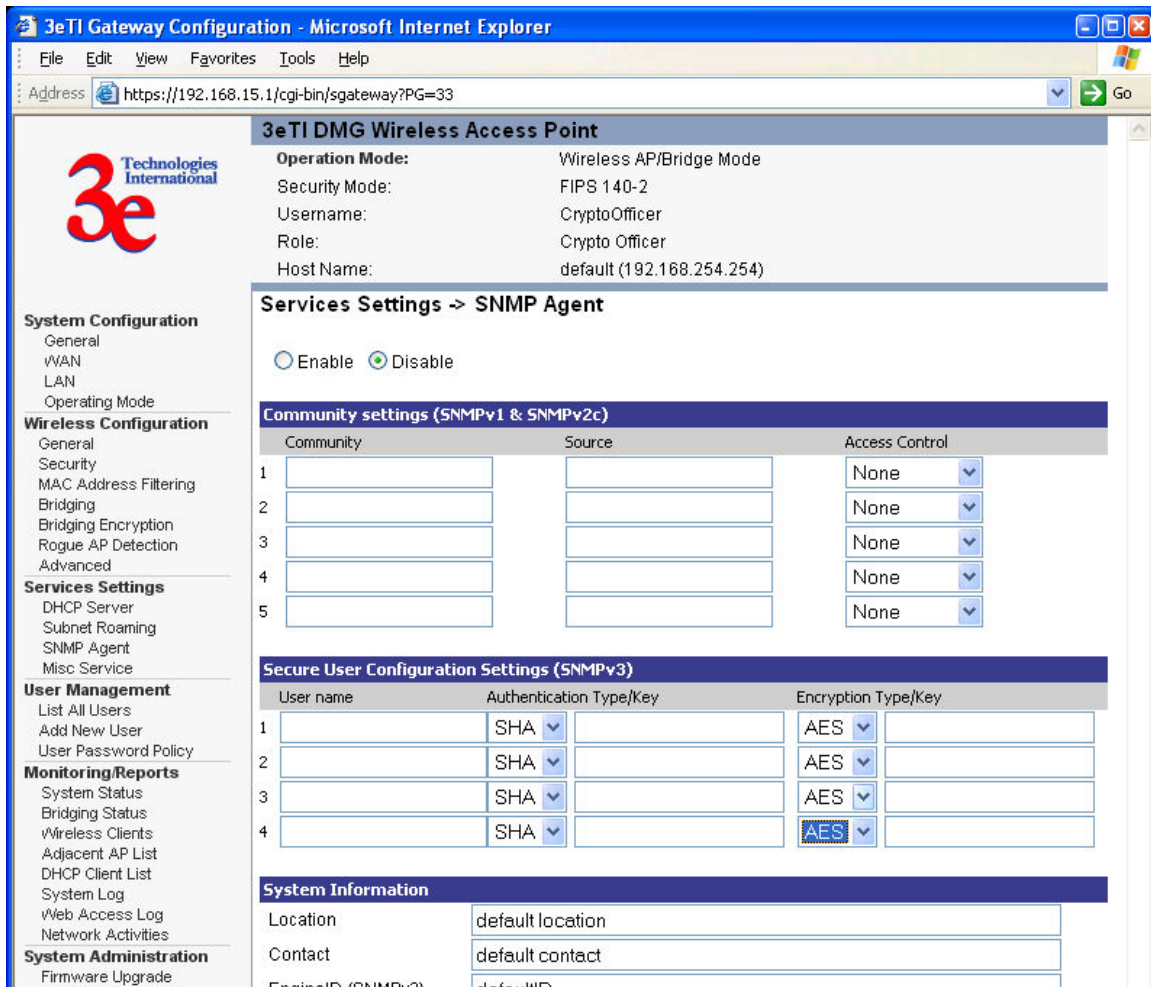
- The service can be enabled or disabled.
- The IP address of coordinator server.



3.3.4.3. SNMP agent

Configures the device to work with the network administrator's Simplified Network Management Protocol station.

- The SNMP agent can be enabled or disabled.
- Community settings.
- Secure user configuration settings
- System information



3eTI Gateway Configuration - Microsoft Internet Explorer

Address: <https://192.168.15.1/cgi-bin/sgateway?PG=33>

3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
 Security Mode: FIPS 140-2
 Username: CryptoOfficer
 Role: Crypto Officer
 Host Name: default (192.168.254.254)

Services Settings → SNMP Agent

☐ Enable ☒ Disable

Community settings (SNMPv1 & SNMPv2c)

Community	Source	Access Control
1		None
2		None
3		None
4		None
5		None

Secure User Configuration Settings (SNMPv3)

User name	Authentication Type/Key	Encryption Type/Key
1	SHA	AES
2	SHA	AES
3	SHA	AES
4	SHA	AES

System Information

Location	default location
Contact	default contact
EngineID (SNMPv3)	defaultID

System Configuration

- General
- WAN
- LAN
- Operating Mode

Wireless Configuration

- General
- Security
- MAC Address Filtering
- Bridging
- Bridging Encryption
- Rogue AP Detection
- Advanced

Services Settings

- DHCP Server
- Subnet Roaming
- SNMP Agent
- Misc Service

User Management

- List All Users
- Add New User
- User Password Policy

Monitoring/Reports

- System Status
- Bridging Status
- Wireless Clients
- Adjacent AP List
- DHCP Client List
- System Log
- Web Access Log
- Network Activities

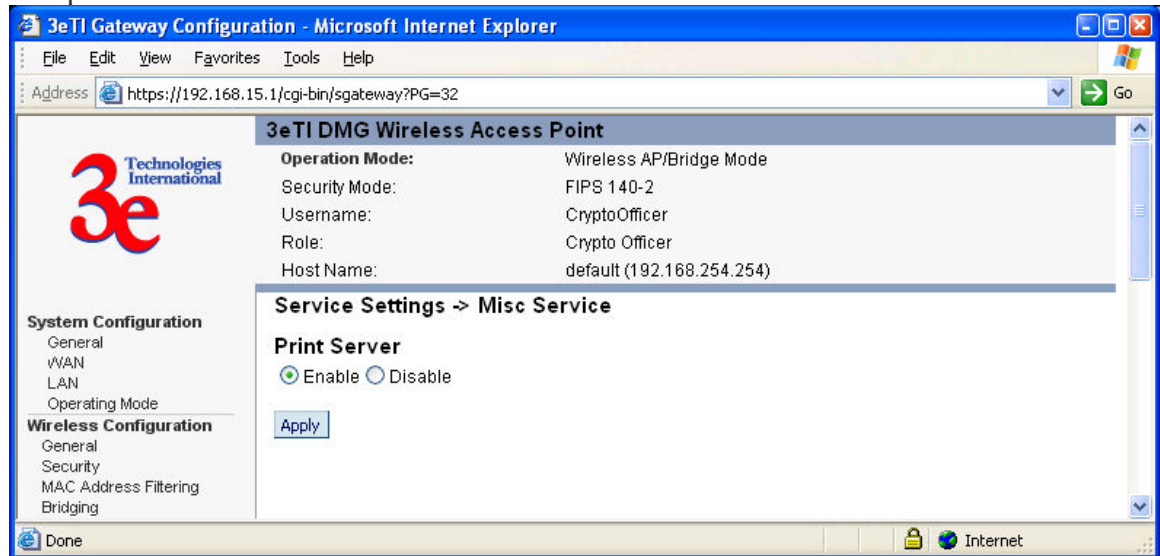
System Administration

- Firmware Upgrade

3.3.4.4. Misc service

Configures the print server service for sharing the printer (only for 525A and 519).

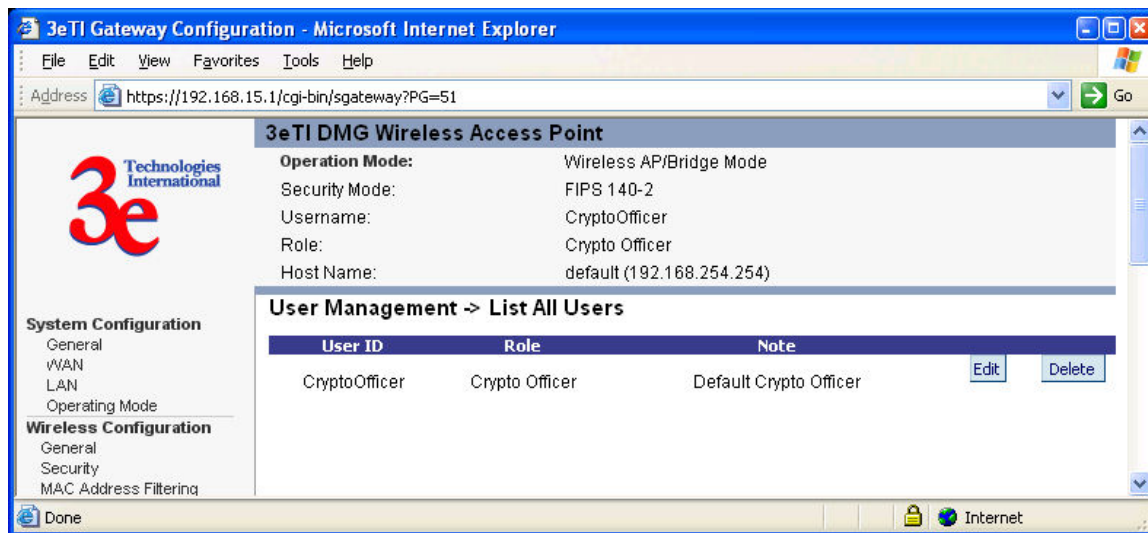
- The print service can be enabled or disabled.



3.3.5. User Management

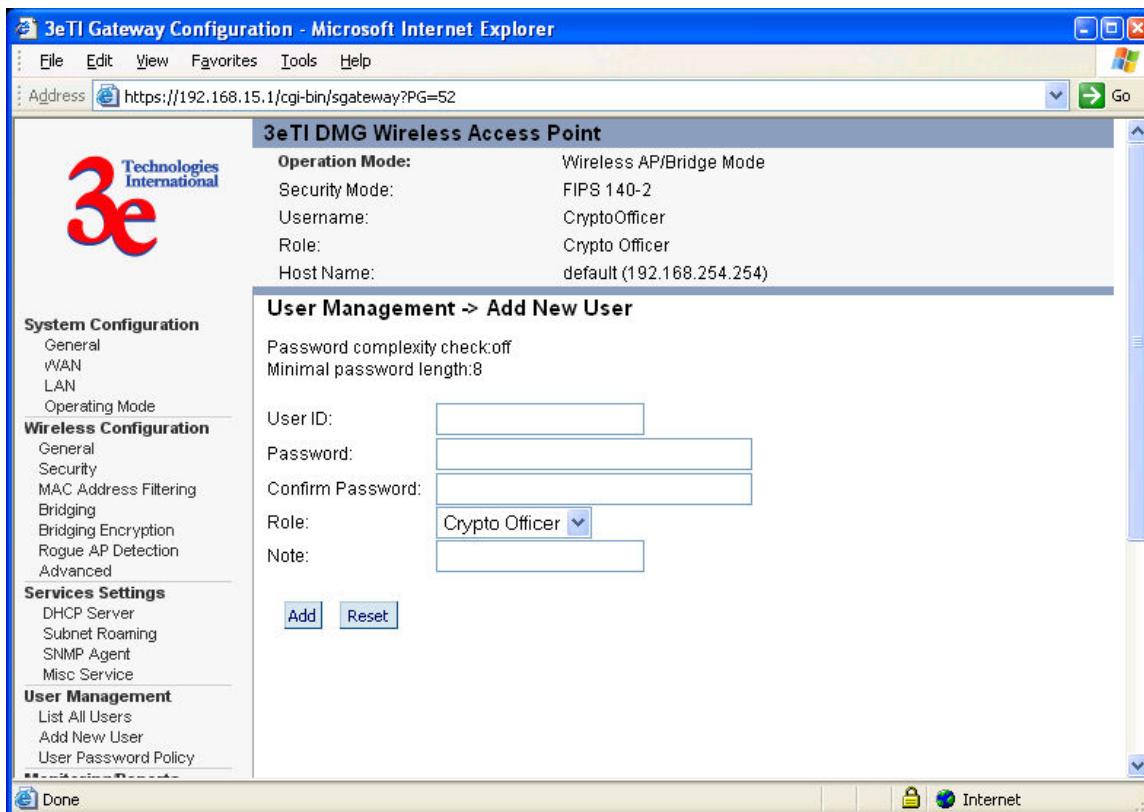
3.3.5.1. List All Users

A list of the Crypto Officer and Administrator(s) by user ID is included.



3.3.5.2. Add New User

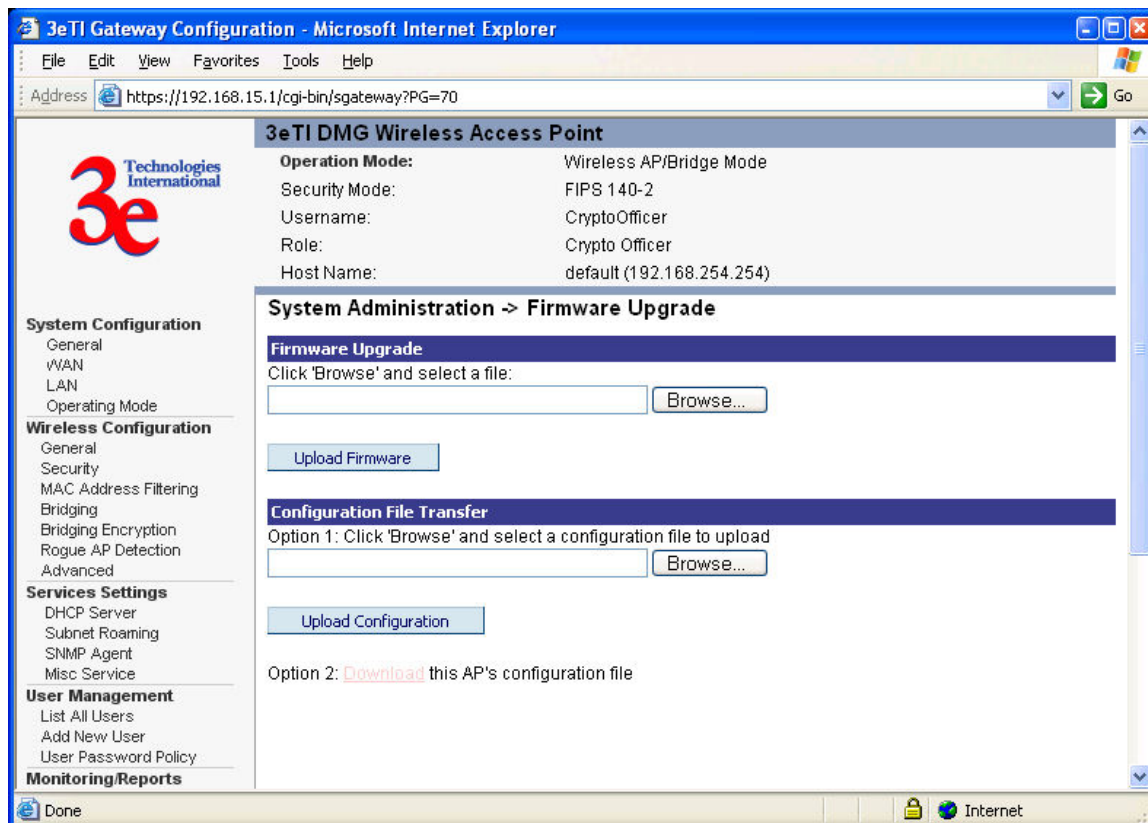
Only Crypto Officer is able to add a new user (Administrator) to the Gateway.



3.3.6. System Administration

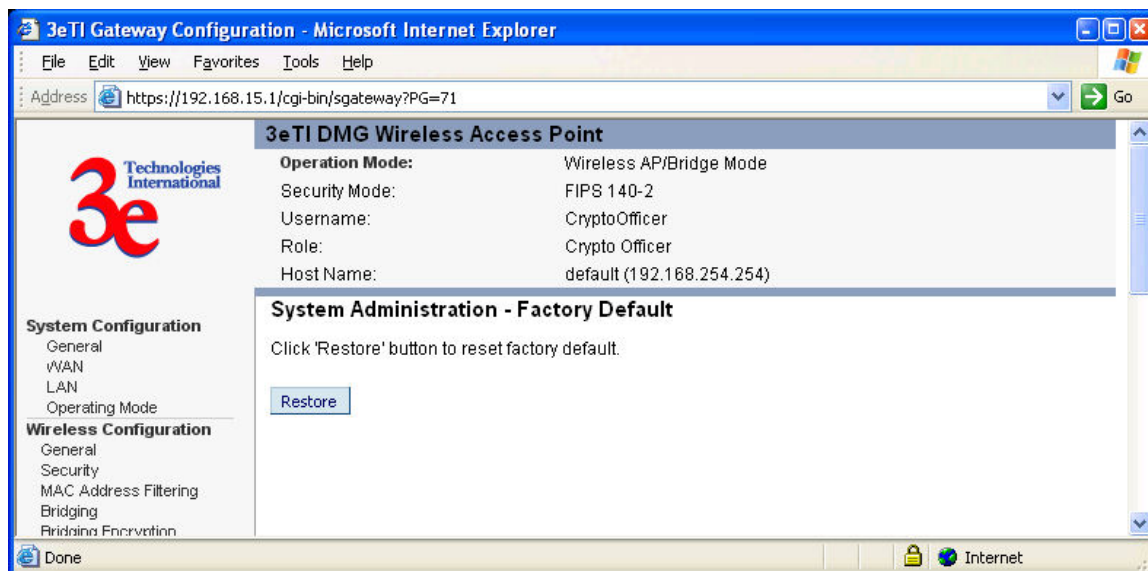
3.3.6.1. Firmware Upgrade

Only the Crypto Officer can select a file to upload for firmware upgrade.



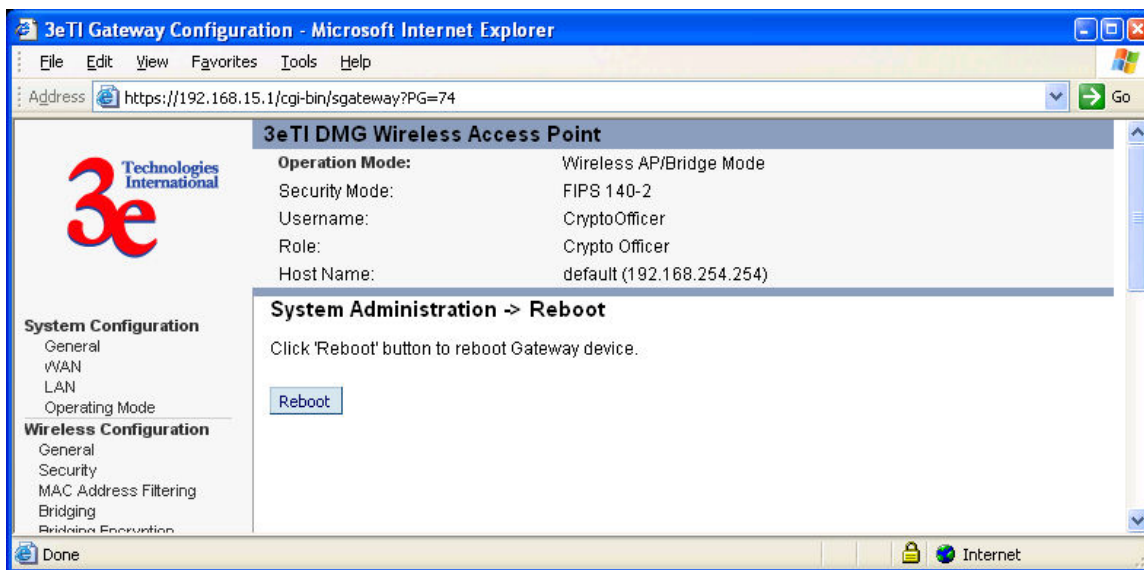
3.3.6.2. Factory Default

Only the Crypto Officer can restore the Gateway to the factory default settings. For the Gateways a Reset switch, which is not accessible from outside, is provided on the motherboard of the module that achieves the same goal. When this switch is depressed for 10 seconds or longer it resets the module back to factory default settings.



3.3.6.3. Reboot

Both Crypto Officer and Administrators can reboot the Gateway.



4. Security Relevant Data Items

This section specifies the 3e-DMG's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the 3e-DMG.

4.1. Cryptographic Algorithms

The 3e-DMG supports the following FIPS Approved cryptographic algorithms:

- TDES (ECB, CBC modes; 192-bit keysize)
- AES (ECB mode; 128, 192, 256-bit keysizes)
- SHA-1
- HMAC-SHA1
- FIPS 186-2 (Appendix 3.1 and 3.3) PRNG

The 3e-DMG also supports the following non-FIPS cryptographic algorithms:

- Diffie Hellman (1024-bit modulus)⁺
- RSA decrypt (PKCS#1) for key un-wrapping.⁺
- RC4 (used in WEP)
- MD5 hashing (used in MS-CHAP for PPPoE and SNMP agent)
- AES (CFB mode; 128 bit keysize) (used in SNMP v3)⁺
- DES (CBC) (used in SNMP v3)⁺

Note 1: RC4 and MD5 are only used in non-FIPS mode

Note 2: The data encrypted using AES (CFB mode only) and DES are considered to be in plaintext for FIPS purposes because the encryption keys to these algorithms are derived from pass-phrases.

4.2 Self-tests

4.2.1 Power-up Self-tests

3DES ECB - encrypt/decrypt KAT

3DES CBC - encrypt/decrypt KAT

AES ECB - encrypt/decrypt KAT

SHA-1 KAT

HMAC-SHA-1 KAT

⁺ Used in FIPS mode of operation.

FIPS 186-2 (Appendix 3.1, 3.3) KAT

Integrity Test for firmware

4.2.2 Conditional Self-tests

CRNGT for Approved PRNG

CRNGT for non-Approved PRNG (Open SSL based)

Bypass Test

Firmware Load Test

4.2.3 Critical Functions tests

DH pairwise consistency test (power-up)

4.3 Cryptographic Keys and SRDIs

The 3e-DMG contains the following security relevant data items:

Security Relevant Data Items	SRDI Description	Key Zero-izing
AES or 3DES Static Key	Data encryption/decryption using an AES static key (128, 192, or 256-bits) or 3DES static key (192-bits)	N/A The key is stored encrypted.
AES or 3DES Dynamic Broadcast Key	Data encryption/decryption using an internally generated AES key (128, 192, or 256-bits) or 3DES (192-bits)	Key is zero-ized on a power-cycle, CryptoOfficer changes from DKE mode to static key mode, or re-applies DKE mode.
AES or 3DES Dynamic Unicast Key	Data encryption/decryption using an dynamically exchanged AES key (128, 192, or 256-bits) or 3DES (192-bits)	Key is zero-ized on a power-cycle, CryptoOfficer changes from DKE mode to static key mode, DKE mode is re-applied, or a client disassociates.
AES Internal Key	Used to encrypt configuration file	The key can be zeroized by powering down the module and upgrading the firmware
AES Post-Authentication Key	AES Key used to decrypt the 3DES/AES Dynamic Unicast Key	The key is zeroized after the unicast key (encrypted by this AES key) is decrypted by the module.

HMAC SHA-1 Key	Key used to verify firmware integrity and authenticity during firmware upgrade	The key is zeroized by upgrading firmware twice.
HMAC SHA-1 Shared Secret	Secret used to authenticate the Security Server	N/A. The key is stored encrypted
TLS Session Key	TDES key used to encrypt/decrypt configuration sessions (via HTTPS)	This key is zeroized when the module is power cycled.
RSA Private Key	Used to decrypt pre-master key in TLS negotiation	The key is zeroized by setting the module to factory default and upgrading the firmware twice.
Crypto-officer password	CO Password	This password can be zeroized by setting the module to factory default.
Administrator password	Administrator Password	This password can be zeroized by setting the module to factory default.
HMAC-SHA-1 SNMP key	This key is used to authenticate SNMP packets.	The key is zeroized by setting the module to Factory Default.
Diffie-Hellman Private exponent	This exponent is used to negotiate the AES post authentication key with the security server.	The key is zeroized after the unicast key (encrypted by the established AES key) is decrypted by the module.

4.4 Access Control Policy

The 3e-DMG maintains and enforces the access control policy for each SRDI stored within the module. These access control policies cannot be changed or modified by any role within the module. The permissions are categorized as a set of three separate permissions: read (R), write (W), execute (E). If no permission is listed, then the operator cannot access the SRDI. The following table defines the access that an operator has to each SRDI and through which services.

3e-DMG SRDI Roles and Services Access Policy	Security Relevant Data Item													
	AES or TDES Static Key													
	AES or TDES Dynamic Broadcast													
	AES or TDES Dynamic Unicast													
	AES Internal Key													
	AES Post-authentication Key													
	HMAC SHA-1 Key													
	HMAC SHA-1 Shared Secret													
	TLS Session Key													
	RSA Private Key													
	Crypto-officer password													
	Administrator Password													
	HMAC SHA-1 SNMP key													
	Diffie-Hellman Private exponent													
Role/Service														
Crypto-officer Role														

System Configuration				E				E	E				
Wireless Configuration	W			E			W	E	E				
Service Settings				E				E	E			W	
User Management								E	E	W	W		
Monitoring/Reporting				E				E	E				
System Administration				E		E		E	E				
Administrator Role													
System Configuration				E				E	E				
Wireless Configuration				E				E	E				
Service Settings				E				E	E			W	
User Management								E	E		W		
Monitoring/Reporting				E				E	E				
System Administration				E				E	E				
User Role													
Sending data	E	E	E										
Authentication Server Role													
Provides authentication			W		W		E						W

5. Operational Environment

This section does not apply since the module is operated in a non-modifiable operating environment.

6. EMI/EMC

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

7. Design Assurance

3eTI implements a configuration management (CM) system for the 3e-DMG, 3e-DMG components, and associated 3e-DMG documentation. The CM infrastructure is based on the UNIX CM utility “CVS”.

8. Mitigation of Other Attacks

The module does not claim to mitigate any specific attacks.